Oracle® Communications Mobile Synchronization Gateway

System Administrator's Guide

Release 8.0

E67473-01

August 2016

ORACLE®

Oracle Communications Mobile Synchronization Gateway System Administrator's Guide, Release 8.0

E67473-01

Contents

Preface

This guide explains how to administer Oracle Communications Mobile Synchronization Gateway and its accompanying software components.

Audience

This document is intended for system administrators whose responsibility includes Mobile Synchronization Gateway. This guide assumes you are familiar with the following topics:

- Oracle Communications Calendar Server, Oracle Communications Contacts Server, and Oracle Communications Messaging Server protocols
- Oracle GlassFish Server
- Oracle Directory Server Enterprise Edition and LDAP
- System administration and networking
- General deployment architectures

Related Documents

For more information, see the following documents in the Mobile Synchronization Gateway documentation set:

- *Mobile Synchronization Gateway Installation and Configuration Guide*: Provides instructions for installing and configuring Mobile Synchronization Gateway.
- *Mobile Synchronization Gateway Release Notes*: Describes the new features, fixes, known issues, troubleshooting tips, and required third-party products and licensing.
- *Mobile Synchronization Gateway Security Guide*: Provides guidelines and recommendations for setting up Mobile Synchronization Gateway in a secure configuration.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit

http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

1

Mobile Synchronization Gateway Administration Overview

This chapter describes the basic Mobile Synchronization Gateway administration tasks and tools used to perform those tasks.

Overview of Mobile Synchronization Gateway Administration Tasks

A Mobile Synchronization Gateway administrator is responsible for the day-to-day tasks of maintaining and managing Mobile Synchronization Gateway and its users. The tasks also include managing Mobile Synchronization Gateway components, Oracle GlassFish Server, and potentially other Unified Communications Suite components.

You perform the following tasks as a Mobile Synchronization Gateway administrator:

- Stopping and starting Mobile Synchronization Gateway
- Configuring Mobile Synchronization Gateway for direct push
- Monitoring Mobile Synchronization Gateway
- Tuning Mobile Synchronization Gateway performance
- Troubleshooting Mobile Synchronization Gateway

About Mobile Synchronization Gateway Administration Tools

Mobile Synchronization Gateway is deployed on a GlassFish Server domain. You use the GlassFish Server Administration Console and **asadmin** command to manage the Mobile Synchronization Gateway web container. See the GlassFish Server documentation for more information.

Mobile Synchronization Gateway provides several command-line utilities for administering the server. These utilities run under the umbrella command, **mgadmin**. For more information, see "Mobile Synchronization Gateway Command-Line Utilities".

Directory Placeholders Used in This Guide

Table 1–1 lists the placeholders that are used in this guide:

Table 1–1 Mobile Synchronization Gateway Directory Placeholders

Placeholder	Directory
MobileSyncGateway_home	Specifies the installation location for the Mobile Synchronization Gateway software. The default is **/opt/sun/comms/mobile**.
GlassFish_home	Specifies the installation location for the Oracle GlassFish Server software. The default is **/opt/glassfish3/glassfish**.
MessagingServer_home	Specifies the installation location for the Oracle Communications Messaging Server software. The default is **/opt/sun/comms/messaging64**.

2

Stopping and Starting Mobile Synchronization Gateway

This chapter describes how to stop and start Oracle Communications Mobile Synchronization Gateway services.

Stopping and Starting Mobile Synchronization Gateway

To stop and start the Mobile Synchronization Gateway process, you use the **asadmin stop-domain** and **asadmin start-domain** commands to stop and start the Oracle GlassFish Server container in which Mobile Synchronization Gateway is deployed. The following examples assume a default GlassFish Server installation with Mobile Synchronization Gateway deployed in **domain1**.

- To stop Mobile Synchronization Gateway:

  ```
  GlassFish_home/bin/asadmin stop-domain domain1
  ```

- To start Mobile Synchronization Gateway:

  ```
  GlassFish_home/bin/asadmin start-domain domain1
  ```

3

Managing Mobile Synchronization Gateway

This chapter provides details on managing and tuning Oracle Communications Mobile Synchronization Gateway.

Administering GlassFish Server

Mobile Synchronization Gateway depends on Oracle GlassFish Server as a web container. See the Oracle GlassFish Server 3 documentation for details on administering GlassFish Server.

The following Glassfish Server documentation will help you get started:

- "Certificates and SSL" in *Glassfish Server Security Guide*
- "asadmin Utility" in *Glassfish Server Administration Guide*

Using Mobile Synchronization Gateway Utilities

Mobile Synchronization Gateway provides several command-line utilities for server administration. These utilities run under the umbrella command, **mgadmin**, which is a simple shell script. By default, the **mgadmin** utility is installed in the *MobileSyncGateway_home*/**sbin** directory with user or group **bin/bin** permissions. See "Mobile Synchronization Gateway Command-Line Utilities" for more information.

Managing Logging

Managing logging includes:

- Logging Mobile Synchronization Gateway Information to the GlassFish Server Log File
- Configuring Logging
- Using the commands Log

Overview of Mobile Synchronization Gateway Logging

Mobile Synchronization Gateway maintains the following types of log files:

- **commands**: Stores information about requests that are sent to the server and information related to each operation performed to satisfy those requests. The **commands** log contains servlet and core operation classes entries that are designed to help you monitor requests to the server and help diagnose problems. See "Using the commands Log" for more information on the **commands** log.

- **errors**: Stores error and debug-level information that is supplied by the server for use in diagnosing problems.
- **telemetry**: Stores entire Mobile Synchronization Gateway servlet request and response transcripts.

Each log file has its own configuration parameters that control the log file location, maximum size, log level, and number of files allowed.

Log files are created with a suffix of *.number*, for example, **commands.0**, **commands.1**, and so on. The log file numbered **.0** is the newest, the log file numbered **.1** is next newest, and so on. When a log file is filled to its maximum configured size, the logging system increments each of the existing log file suffixes to the next higher number, starting with the highest. If the number of log files reaches the configured maximum, the highest numbered log file is deleted and the next higher takes its place.

For example, Mobile Synchronization Gateway is started for the first time and you have configured the maximum number of log files at 10. The logging system begins writing messages to the log file with the **.0** suffix. When the **.0** log file is filled to capacity, the logging system increments its suffix to the next higher number and the file becomes **.1**. The logging system then creates a new **.0** log file and begins writing messages to it. When the **.0** file become full, the logging system increments the **.1** file to **.2**, increments the **.0** file to **.1**, and creates a a new **.0** file. This process continues until the maximum number of configured log files is reached. When that happens, the logging system deletes the highest numbered (oldest) log file, **.9**, increments each of the lower numbered files' suffixes, and creates a new **.0** log file.

The Mobile Synchronization Gateway log files are kept separate from the GlassFish Server log files. The GlassFish Server log files are maintained in the *GlassFish_home*/**domains/***domain_name*/**logs** directory, for example, **/opt/glassfish3/glassfish/domains/domain1/logs**. Even though the container's log file is the root log file, by default, information that is logged to the Mobile Synchronization Gateway's log files is not logged to the container's log file.

Logging Mobile Synchronization Gateway Information to the GlassFish Server Log File

The Mobile Synchronization Gateway **logToParent** flag is **false** by default, preventing logging of information to the GlassFish Server log file.

To log Mobile Synchronization Gateway information to both the GlassFish Server log file (**server.log**) and the Mobile Synchronization Gateway log file (**commands.0**):

- Set the **log.mg.commands.logtoparent** parameter to **true**:

```
mgadmin config modify -u admin -o log.mg.commands.logtoparent -v true
```

Configuring Logging

Use the **mgadmin** command to configure Mobile Synchronization Gateway logging configuration parameters as shown in Table 3–1.

name can be **commands**, **errors**, or **telemetry**, depending on the type of logging you want to configure; use **errors** to configure Mobile Synchronization Gateway error logging. **SEVERE** and **WARNING** messages need immediate attention. **FINE**, **FINER**, and **FINEST** messages are usually informational only, but can provide more context for troubleshooting when accompanying **SEVERE** and **WARNING** messages.

For more information about the logging configuration parameters and their default values, see "Mobile Synchronization Gateway Configuration Files and Parameters".

Table 3–1 Mobile Synchronization Gateway Log File Parameters

Parameter	Description
log.mg.*name***.logdir**	Specifies the log file directory path
log.mg.*name***.loglevel**	Specifies the log level: ■ **OFF**: No information is logged. ■ **SEVERE**: Logs catastrophic errors. ■ **WARNING**: Logs major errors or exceptions with the system. ■ **INFO**: Logs general informational messages. This is the default level. ■ **FINE**: Logs general debugging and tracing information to show the higher level flow through the code or more detailed information about a problem. ■ **FINER**: Logs more details than **FINE**. ■ **FINEST** or **ALL**: Logs the finest grain details about code flow or problem information. Enabling this level can result in massive amounts of data in the log file, making it hard to parse.
log.mg.*name***.logtoparent**	Enables or disables logging to the GlassFish Server log file. When set to **true**, messages are logged to both the GlassFish Server log file and the Mobile Synchronization Gateway log file. Set to **false** to disable logging to the GlassFish Server log file.
log.mg.*name***.maxlogfiles**	Specifies the maximum number of log files
log.mg.*name***.maxlogfilesize**	Specifies the log file's maximum size

Using the commands Log

The Mobile Synchronization Gateway **commands** log file contains per servlet entries that are designed to help monitor requests to the server and help diagnose problems. The **commands** log file includes the principal account that logged in and what operations were done from that account.

Table 3–2 describes the **command** log fields. The **commands** log records contain two set fields and one variable field.

Table 3–2 commands Log Fields

Field	Description
Time stamp	Identifies when the log entry is created.
Sequence	Specifies a unique number for each request.
Variable	Logs information about the start and end of specific internal server operations. For HTTP commands that are logged from the servlet layers, this field also logs the HTTP request coming in with an **[REQ]**, the HTTP method, URI information, IP address, host name, port, and the user principal information for that request. The corresponding response is marked as **[RES]**, followed by an HTTP status.

Creating the passfile

When running the **mgadmin** command, instead of having to enter passwords at the no-echo prompt, you can supply passwords by using the **password** file. The **password** file is an encrypted "wallet," which holds all passwords that **mgadmin** might use. The **mgadmin passfile** operation creates, deletes, or modifies this **password** file.

To create the passfile:

1. Log in to the Mobile Synchronization Gateway host as **root**.
2. Change to the *MobileSyncGateway_home*/**sbin** directory.
3. Run the **mgadmin passfile create** command and follow the prompts.

Configuring Messaging Server, Calendar Server, and Contacts Server for Direct Push

This section describes how to configure direct push for Oracle Communications Messaging Server, Oracle Communications Calendar Server, and Oracle Communications Contacts Server.

About Direct Push

Microsoft® Exchange ActiveSync direct push technology enables Mobile Synchronization Gateway to keep data on mobile devices synchronized with the data on Messaging Server, Calendar Server, and Contacts Server hosts. Direct push works by mobile devices issuing timed requests for email folder, calendar, and address book changes on the back-end servers. For more information about how direct push works, see the topic about direct push technology on the Microsoft TechNet Library website at:

http://technet.microsoft.com/en-us/library/cc182244.aspx

Direct push operation consists of the following high-level steps:

1. The end user performs an initial synchronizing of the mobile device.
2. The mobile device periodically pings the Mobile Synchronization Gateway host at a client-specified heart beat interval.
3. The back-end host delays its response until one of the following conditions becomes true:
   - The heartbeat time interval is reached (status 1), resulting in no change.
   - A data change occurs, such as new email, deleted email, and so forth (status 2).
   - A folder hierarchy synchronization is required before any individual folder synchronization (status 7).
   - A status indicates various bad commands or syntax errors (status 1 to 8).
   - An event has occurred on a back-end server, such as an event created on Calendar Server, or a contact modified on Contacts Server.

How Mobile Synchronization Gateway Implements Direct Push

To enable direct push, the Mobile Synchronization Gateway implements a synchronization engine. The synchronization engine consists of Java Message Service

(JMS) consumer modules, one for Messaging Server, and one for Calendar Server and Contacts Server.

Direct Push for Calendar Server and Contacts Server

For Calendar Server and Contacts Server, the consumer module within the synchronization engine manages a JMS connection to a "DAV" Message Queue broker. The consumer is also a subscriber to the DAV Message Queue, subscribing on the topic **DavNotificationTopic**. The consumer listens for messages with specific changes that pertain to the user accounts that are actively subscribed to the Mobile Synchronization Gateway server. Certain messages, such as a new calendar was created or a contact was modified, trigger a direct push to the user's device.

Direct Push for Messaging Server

For Messaging Server, the synchronization engine uses a Java Message Queue (JMQ) Event Notification Service (ENS) plug-in. The plug-in publishes messages to a JMQ broker when changes occur to user accounts that are actively subscribed to Mobile Synchronization Gateway. Certain messages, such as a new message arrived or a message was deleted, trigger a direct push to the user's device.

To use direct push for Messaging Server, you must configure Messaging Server to use the following ENS plug-in, and you must set the following options for the plug-in:

- Enable the unauthenticate IMAP extension.
- Set the cache preview length to 600 characters if that option is not already set.
- Create an ENS plug-in named **mgplugin**.
- Create an ENS event key, **enp://127.0.0.1/mgnotify/**, which creates a topic with name **mgnotify**, in the format, **enp://127.0.0.1/***topic*/.
- Enable new message events.
- Enable flag change events such as **changeflag**, **readmsg**, **deletemsg**.
- Disable other events.

> **Note:** Because folder creation and deletion events are always enabled in Messaging Server, you do not need to enable them.

You can configure Messaging Server either by using legacy configuration (**configutil** command) or Unified Configuration (**msconfig** command). Using Unified Configuration enables you to configure the plug-in by simply running a recipe file to set the needed options. In addition, using Unified Configuration recipes saves time by setting all the required options with a single command, and lessens the chance to make configuration mistakes due to typing errors.

Configuring Calendar Server and Contacts Server for Direct Push

To use direct push, ensure that you have configured Calendar Server and Contacts Server to use notifications. For more information, refer to the topic on using notifications in each product's *System Administrator's Guide*.

To configure Mobile Synchronization Gateway for direct push with Calendar Server and Contacts Server:

1. Log in as superuser (**root**) to the Mobile Synchronization Gateway host.

2. Configure direct push for Calendar Server:
   - If Calendar Server is on the local host:

     ```
     mgadmin config modify -o caldav.mqhosturls -v localhost:37676
     ```

   - If Calendar Server is on a remote host:

     ```
     mgadmin config modify -o caldav.mqhosturls -v cs.example.com:37676
     ```

3. Configure direct push for Contacts Server:
   - If Contacts Server is on the local host:

     ```
     mgadmin config modify -o carddav.mqhosturls -v localhost:37676
     ```

   - If Contacts Server is on a remote host:

     ```
     mgadmin config modify -o cardav.mqhosturls -v cs.example.com:37676
     ```

Configuring Messaging Server for Direct Push in Unified Configuration

To configure Messaging Server for Mobile Synchronization Gateway direct push in Unified Configuration:

1. Copy the *MessagingServer_home***/lib/bin/recipes/MobileSyncConfig.rcp** file to the *MessagingServer_home***/data/config/recipes** directory.
2. Run the recipe file:

   ```
   cd MessagingServer_home/bin/
   msconfig run MobileSyncConfig.rcp
   ```

3. Restart Messaging Server.

   ```
   stop-msg
   start-msg
   ```

4. Review the settings for the ENS plug-in.

   ```
   msconfig show *mgplugin*
   ```

Configuring Messaging Server for Direct Push in Legacy Configuration

To configure Messaging Server for Mobile Synchronization Gateway direct push in legacy configuration:

1. Change to the *MessagingServer_home***/bin** directory.
2. Enable the unauthenticate extension:

   ```
   configutil -o service.imap.capability.x_unauthenticate -v 1
   ```

3. Set the cache preview length:

   ```
   configutil -o store.cachepreviewlen -v 600
   ```

4. Create the ENS plug-in and enable notifications:

   ```
   configutil -o local.store.notifyplugin.mgplugin.enseventkey -v
   "enp://127.0.0.1/mgnotify/"
   configutil -o local.store.notifyplugin.mgplugin.newmsg.enable -v 1
   configutil -o local.store.notifyplugin.mgplugin.updatemsg.enable -v 1
   configutil -o local.store.notifyplugin.mgplugin.deletemsg.enable -v 1
   configutil -o local.store.notifyplugin.mgplugin.changeflag.enable -v 1
   ```

```
configutil -o local.store.notifyplugin.mgplugin.readmsg.enable -v 1
configutil -o local.store.notifyplugin.mgplugin.purgemsg.enable -v 0
configutil -o local.store.notifyplugin.mgplugin.loguser.enable -v 0
configutil -o local.store.notifyplugin.mgplugin.OverQuota.enable -v 0
configutil -o local.store.notifyplugin.mgplugin.UnderQuota.enable -v 0
```

5. Append the **mgplugin** plug-in created in the previous step to the list of plug-ins:

```
configutil -o local.store.notifyplugin -v
"/opt/sun/comms/messaging64/lib/libibiff\$mgplugin"
```

6. If you had previously created notification plug-ins, add the new plug-in to the list of existing plug-ins.

   a. Get the list of existing plug-ins:

```
configutil -o local.store.notifyplugin
/opt/sun/comms/messaging64/lib/libjmqnotify$jmq1
```

   b. Add the new **mgplugin** created as an ENS plug-in as **/opt/sun/comms/messaging64/lib/libibiff$mgplugin**. To separate two plug-ins, use the '$' character (usually escaped in most shells). Add the newly created plug-in to the list of existing plug-ins by adding a '$' character after the list of existing plug-ins:

```
configutil -o local.store.notifyplugin -v
"/opt/sun/comms/messaging64/lib/libjmqnotify\$jmq1\$/opt/sun/comms/messagi
ng64/lib/libjmqnotify\$mgplugin"
```

   c. Review the settings for the ENS plug-in:

```
configutil -o local.store.notifyplugin
/opt/sun/comms/messaging64/lib/libjmqnotify$jmq1$/opt/sun/comms/messaging6
4/lib/libjmqnotify$mgplugin
```

7. Restart Messaging Server.

```
stop-msg
start-msg
```

Configuring Address Book Coexistence

You can configure Mobile Synchronization Gateway to support both the legacy Oracle Communications Convergence Personal Address Book (PAB), which uses Web Address Book protocol (WABP), and the Contacts Server address book, which uses the CardDAV protocol. You might need a coexistence phase while you are migrating users from PAB to Contacts Server. For coexistence of address book servers, you configure Mobile Synchronization Gateway to communicate with both Convergence and Contacts Server, and to distinguish between the WABP and CardDAV protocols.

Configuring address book coexistence includes:

- Enabling Communication over Web Address Book Protocol
- Enabling Communication over CardDAV Protocol
- Configuring the Web Address Book Protocol Host
- Keeping Deleted Contacts on the Web Address Book Protocol Host
- Identifying a User's Address Book Service

Enabling Communication over Web Address Book Protocol

To enable the Mobile Synchronization Gateway host to communicate using the Web Address Book Protocol (WABP):

1. Log in to the Mobile Synchronization Gateway host as **root**.
2. Change to the *MobileSyncGateway_home***/sbin** directory.
3. Run the **mgadmin modify config** command for each of the following configuration parameters with the values shown:

   ```
   wabp.enable=true
   wabp.host=fqdn_of_Convergence_host
   wabp.port=443
   wabp.enablessl=true
   wabp.proxyadminid=admin
   wabp.proxyadminpassword=password
   ```

   For example:

   ```
   mgadmin config modify -o wabp.enable -v true
   ```

4. If necessary, restart GlassFish Server, if the **mgadmin config modify** command informs you to do so.

The WABP (Convergence) host must also have WABP enabled. If have not already enabled WABP, do the following:

1. Log in to the WABP (Convergence) host as **root**.
2. Change to the *Convergence_home***/sbin** directory.
3. Run the following **iwcadmin** command:

   ```
   iwcadmin -o ab.enable -v true
   ```

4. Restart GlassFish Server.

Enabling Communication over CardDAV Protocol

To enable the Mobile Synchronization Gateway host to communicate using the CardDAV protocol:

1. Log in to the Mobile Synchronization Gateway host as **root**.
2. Change to the *MobileSyncGateway_home***/sbin** directory.
3. Run the **mgadmin modify config** command for each of the following configuration parameters with the values shown:

   ```
   carddav.enable=true
   carddav.host=fqdn_of_ContactsServer_host
   carddav.port=443
   carddav.enablessl=true
   carddav.proxyadminid=nabmaster
   carddav.proxyadminpassword=password
   ```

   For example:

   ```
   mgadmin config modify -o carddav.enable -v true
   ```

4. If necessary, restart GlassFish Server, if the **mgadmin config modify** command informs you to do so.

Configuring the Web Address Book Protocol Host

You must turn on proxy authentication on the WABP (Convergence) host by running the Convergence **iwcadmin** command for each of the following configuration parameters:

```
auth.ldap.enableproxyauth = true
auth.adminuserlogin.enable = true
```

For example:

```
iwcadmin -o auth.ldap.enableproxyauth -v true
```

For more information about the **iwcadmin** command, see *Convergence System Administrator's Guide*.

Keeping Deleted Contacts on the Web Address Book Protocol Host

Use the Convergence **iwcadmin** command to set each of the following configuration parameters so that Convergence keeps deleted contacts for a certain interval of time (for example, 7 days):

```
ab.pstore.deleteperm = false
ab.purgeinterval = 7
```

For example:

```
iwcadmin -o ab.pstore.deleteperm -v false
```

For more information about the **iwcadmin** command, see *Convergence System Administrator's Guide*.

Identifying a User's Address Book Service

When both Personal Address Book and Contacts Server are enabled, Mobile Synchronization Gateway needs a way to determine whether users have their address book data stored on the WABP (Convergence) host or the CardDAV (Contacts Server) host. To do so, Mobile Synchronization Gateway searches the Directory Server for a particular LDAP attribute specified by the **mgcore.ldapattr.carddavuserattr** configuration parameter. This parameter contains the LDAP attribute that must be present in a user's LDAP entry for it to be considered a CardDAV user. The default value is **nabStore**.

To change the **mgcore.ldapattr.carddavuserattr** configuration parameter:

1. Log in to the Mobile Synchronization Gateway host as **root**.
2. Change to the *MobileSyncGateway_home***/sbin** directory.
3. Run the following command:

   ```
   mgadmin config modify -o mgcore.ldapattr.carddavuserattr -v ldap_attribute
   ```

Enabling and Disabling Users to Use Mobile Synchronization Gateway

You can enable and disable LDAP users and domains for Mobile Synchronization Gateway service by setting the **mgStatus** LDAP attribute.

By default, if you provision users for email and uniqueID attributes, users have a status of **active**. The **active** status enables users to access Mobile Synchronization

Gateway services. To deny Mobile Synchronization Gateway services to users, you specify a value of either **inactive** or **deleted** for the users's **mgStatus** attribute.

To change the user's **mgStatus** attribute, use your site's preferred LDAP tool, such as **ldapmodify**.

mgStatus Attribute Schema Reference

Absence of the **mgStatus** attribute or a value of **active** indicates active status. A value of **removed**, **deleted**, or **inactive** disables the Mobile Synchronization Gateway service. Any other value enables the service, but this is not recommended. Table 3–3 summarizes the **mgStatus** attribute.

Table 3–3 mgStatus Attribute

Item	Description
Origin	Mobile Synchronization Gateway 8.0
Syntax	cis, single-valued
Object Classes	**mgDomain** and **mgUser**
OID	2.16.840.1.113894.1009.1.109.0.1001.1.1

Tuning the Mobile Synchronization Gateway Deployment

Tuning your Mobile Synchronization Gateway deployment includes:

- Tuning Mobile Synchronization Gateway Logging
- Tuning GlassFish Server

Tuning Mobile Synchronization Gateway Logging

The Mobile Synchronization Gateway telemetry logging function is I/O intensive. For optimal performance, disable the telemetry logs.

To disable telemetry logging:

1. Log in to the Mobile Synchronization Gateway host as **root**.
2. Change to the *MobileSyncGateway_home***/sbin** directory.
3. Run the following command:

```
mgadmin config modify -o mgcore.telemetry.forcetelemetry -v false
```

Tuning GlassFish Server

The following GlassFish Server configurations are for a medium-sized deployment. Adjust the values accordingly for your deployment.

Set the following Java Virtual Machine (JVM) heap memory size options:

- Minimum 500MB, (**-Xms**)
- Maximum 2 GB (**-Xmx**)

For information on how to set JVM options, see the topic on administering JVM options in *Oracle GlassFish Server 3.1 Administration Guide*.

Set the following thread pool sizes for **http-thread-pool**:

- Minimum thread pool size: 500

- Maximum thread pool size: 1500

Add the following parameters to the **/etc/rc.d/rc.local** file that gets executed during system startup:

```
echo "65535" > /proc/sys/fs/file-max
echo 1024 25000 > /proc/sys/net/ipv4/ip_local_port_range
echo 2621143 > /proc/sys/net/core/rmem_max
echo 262143 > /proc/sys/net/core/rmem_default
```

The first parameter increases the number of file descriptors. The next parameter makes more local ports available. The last two parameters increase the memory available with socket buffers.

For more information on tuning GlassFish Server, see *Oracle GlassFish Server 3.1 Performance Tuning Guide*.

4

Monitoring Mobile Synchronization Gateway

This chapter provides details on monitoring Oracle Communications Mobile Synchronization Gateway.

About Monitoring Mobile Synchronization Gateway

Mobile Synchronization Gateway uses a managed bean (MBean) created in Oracle GlassFish Server to collect monitoring data. By using the GlassFish Server's Java Management Extension (JMX) interface, you can then access this data by using a JMX-compliant client. The JMX client connects to the platform's MBeanServer by using a JMX Service URL. Once a client connects to the MBeanServer, it uses the Mobile Synchronization Gateway monitoring MBean object name to access the MBean's attributes.

Mobile Synchronization Gateway Monitoring Attributes

This section describes the attributes of the Mobile Synchronization Gateway monitoring MBean object name, **com.sun.comms.mobile.eas:type=monitor**.

General Monitoring Attributes

Table 4–1 describes the general monitoring attributes.

Table 4–1 General Monitoring Attributes

Name	Type	Description
FailedLogins	Integer	The number of failed login attempts since the server was started.
MQBackends	TabularType Map<*K*,*V*> TabularData (BackendConnectionData)	A dynamic collection of connection status data of back-end hosts, provided in a Map interface, that is, Map<*String backendID*, *BackendRTData rtData*>.
BackendRTData	TabularType Map<*K*,*V*> TabularData (BackendRTData)	A dynamic collection of response time data of back-end connections, provided in a Map interface, that is, Map<*String backendID*, *BackendRTData rtData*>.

Mobile Synchronization Gateway Back-End Host Attributes

Table 4–2 describes the Mobile Synchronization Gateway back-end host monitoring attributes.

Table 4–2 Back-End Host Monitoring Attributes

Name	Type	Description
backendID	String	Name ID of this back-end, in the format of *BackendType-HostName*. For example, a Messaging Server host providing an IMAP service looks like the following: **IMAP-sc111.example.com**
hostUri	String	URI of the host, for example, **sc111.example.com:7676**.
message	String	Optional exception or informational message from this back-end host.
connectionStatus	Integer	The standard integer code that enumerates the status of the back-end host. The possible values are: ■ **600** - The server is up. ■ **601** - The server is down. ■ **605** - The server failed to start. ■ **606** - There was an error while trying to get the status of the services.
timestamp	Long	The system time that this JMX request was issued.

Back-End Database Response Times Attributes

Table 4–3 describes the back-end database average response time monitoring attributes.

Table 4–3 Back-End Database Average Response Times Monitoring Attributes

Name	Type	Description
backendID	String	Name ID of this back-end, in the format of *BackendType-HostName*. For example, a Messaging Server host providing an IMAP service looks like the following: **IMAP-sc111.example.com**
message	String	Optional exception or informational message from this back-end host.
resptime	Long	Response time of simple back-end host requests in milliseconds.
timestamp	Long	The system time at which this request was issued.

Using a Java Management Extension Client to Access the Monitoring Data

Mobile Synchronization Gateway itself does not provide a client to access the monitoring data. Instead, you can use any Java Management Extension (JMX) client.

To access the monitoring data, a JMX client needs the following information:

- GlassFish Server host name or IP address
- GlassFish Server administration port number
- GlassFish Server administrative user name and password
- MBean ObjectName, which is **com.sun.comms.mobile.eas:type=monitor**
- Attribute names

You connect a JMX client to the GlassFish Server's MBeanServer by using a JMX Service URL of the following form:

```
service:jmx:rmi:///jndi/rmi://host:port/jmxrmi
```

where:

- *host* is the name or IP address of the GlassFish Server
- *port* is the GlassFish Server administration port number

More information on JMX and JMX clients is available on the Java documentation web site at:

https://docs.oracle.com/javase/8/docs/technotes/guides/jmx/

Using the responsetime Script

In addition to using monitoring data gathered by the Mobile Synchronization Gateway monitoring MBean, you can also check the health of your hosts by using the Mobile Synchronization Gateway supplied **responsetime** script. This script sends a set of basic requests to Mobile Synchronization Gateway and measures the amount of time needed to process those requests. When the **responsetime** script shows a spike or a large increase in response time, this indicates a potential issue with Mobile Synchronization Gateway that must be addressed.

To run the **responsetime** script, you must provide the server type (**mobilesync_gateway**), the GlassFish Server host name and port, and an LDAP user account to run the script. When the script finishes, it displays the number of milliseconds needed to run the series of requests to **stdout**. When the script encounters no problems, it returns an exit status of **0**. If the script encounters a problem, it returns an exit status of **1** to **stderr**. See "responsetime Script Error Codes" for a list of error codes and descriptions.

responsetime Script Syntax

Use the **responsetime** script to check the health of your Mobile Synchronization Gateway hosts.

Location

MobileSyncGateway_home/**sbin**

General Syntax

```
responsetime -t mobilesync_gateway -H host -p port [-s path_of_truststore]
             [-x context_root] [-L locale] [-h]
```

Table 4–4 describes the options.

Table 4–4 responsetime Script Options

Option	Description
-t	Specifies to monitor Mobile Synchronization Gateway (**mobilesync_gateway**).
-H	Specifies the GlassFish Server host name.
-p	Specifies the GlassFish Server administrative port.
-s	Specifies the path to the truststore file, if a secure connection is used.
-x	Specifies the context root for Mobile Synchronization Gateway. The default is **/** (root).

Table 4–4 (Cont.) responsetime Script Options

Option	Description
-L	Specifies the language locale to use to display messages. The format is *LL_CC_VV*, where: ■ *LL* is the language code. ■ *CC* is the country code. ■ *VV* is the variant.
-h	Displays usage help.

The **responsetime** script requires that you stream the following user name and password, each on a separate line, to the script by using **stdin**:

- **RT_USER=***user*
- **RT_PWD=***password*

The **responsetime** script uses HTTP to perform a folder synchronization with Mobile Synchronization Gateway then measures the amount of time needed to process the request.

For information on creating a dedicated user account for **RT_USER**, see "Creating a Dedicated User Account for the responsetime Script".

responsetime Script Error Codes

Table 4–5 describes the **responsetime** script error codes and descriptions.

Table 4–5 responsetime Script Error Codes

Error Code	String	Description
200	Ok	The request succeeded and the amount of time, in milliseconds, is displayed to **stdout**.
201	Application server is down.	The **responsetime** script cannot connect to the GlassFish Server host.
202	Mobile Synchronization Gateway is down or server path not found.	The **responsetime** program had trouble sending a request to the GlassFish Server host.
204	Login failure.	A problem occurred when trying to log in to the GlassFish Server host.
205	Invalid user name or password.	Either the user name or the password was invalid.
206	Invalid server type.	The value of the **-t** option provided was invalid.
207	Response Time request failed.	A problem occurred when a request was made to the GlassFish Server.
208	Unable to find truststore file.	The truststore file was not found or could not be accessed.
209	Unable to create resource.	A problem occurred when creating the monitoring event.

Table 4–5 (Cont.) responsetime Script Error Codes

Error Code	String	Description
210	Unable to locate or open messages resource bundle.	A problem occurred when accessing the localization resource bundle.
211	Invalid option:	An invalid option was entered on the command line.
212	The "{0}" option is required.	A required option was not entered on the command line. The "{0}" string is replaced in the message with the name of the missing option.

responsetime Script Example

The following example shows how to invoke the **responsetime** script and run it by using **csrtuser** as **RT_USER**.

```
#!/bin/sh
#
echo "RT_USER=csrtuser\nRT_PWD=password" | sbin/responsetime -t mobilesync_gateway
-H sc11.example.com -p 8080 -x /

bash> example_csrt.sh
1374
bash>
```

Creating a Dedicated User Account for the responsetime Script

The **responsetime** script requires a user account in LDAP to be specified in the **RT_USER** variable. You should create a dedicated user account for the **responsetime** script to use. Create this user by using the Mobile Synchronization Gateway **config-rtuser** script, which is located in the *MobileSyncGateway_home*/**sbin** directory. The **config-rtuser** script creates the user in LDAP.

To create a dedicated user for the **responsetime** script by using the **config-rtuser** script:

1. Log in to the Mobile Synchronization Gateway host as **root**.
2. Change to the *MobileSyncGateway_home*/**sbin** directory.
3. Run the **config-rtuser** script:

   ```
   config-rtuser
   ```

4. Respond to the prompts for user account and password, LDAP unique identifier attribute, Directory Manager password, and GlassFish Server administrative password.
5. When prompted to proceed, type **Y**.

   The script runs the **ldapmodify** command to create the user account.

5

Troubleshooting Mobile Synchronization Gateway

This chapter describes troubleshooting strategies for Oracle Communications Mobile Synchronization Gateway.

Enabling Telemetry Logging

To troubleshoot issues with a particular user or client, it is useful to log all protocol interactions. You can force all telemetry logs by setting the **mgcore.telemetry.forcetelemetry** parameter to **true**. Do not use this setting unless required as it generates lots of data.

To set the **mgcore.telemetry.forcetelemetry** parameter to **true**:

```
mgadmin config modify -o mgcore.telemetry.forcetelemetry -v true
```

To filter on specific email addresses, set the **mgcore.telemetry.filter** parameter:

```
mgadmin config modify -o mgcore.telemetry.filter -v space_separated_list_of_email_addresses
```

Troubleshooting Connecting to Convergence

If Convergence clients are experiencing problems connecting to Mobile Synchronization Gateway, check the logs for errors such as "WABP Error Code 1001" or "WABP user not connecting." The problem could be that Convergence has not been properly configured for proxy authentication.

To enable Convergence for proxy authentication:

1. Log in to the Convergence host as **root**.
2. Set the **auth.ldap.enableproxyauth** configuration parameter for proxy authentication:

   ```
   iwcadmin -u admin -o auth.ldap.enableproxyauth -v true
   ```

3. Set the **auth.adminuserlogin.enable** configuration parameter to allow proxy administrators to log in:

   ```
   iwcadmin -u admin -o auth.adminuserlogin.enable -v true
   ```

Troubleshooting Back-End Services

This section provides information to help you troubleshoot the email, calendar, and WABP back-end services to which Mobile Synchronization Gateway connects.

General Back-End Services Troubleshooting

If Mobile Synchronization Gateway is experiencing problems with one or more of the back-end services, disable that service (or services) on the Mobile Synchronization Gateway host. Then restart Mobile Synchronization Gateway. In this way, you can begin to isolate the problem while continuing to run unaffected services.

For example, if you have a deployment that consists of email, calendar, and WABP services, and you think the WAPBP service is causing problems, disable WABP on the Mobile Synchronization Gateway host then restart Mobile Synchronization Gateway. If the email and calendar services function correctly, you can then investigate the problem with the WABP service, while keeping the email and calendar services available.

To disable a service on Mobile Synchronization Gateway, use the **mgadmin** command to set the service's ***.enable** configuration parameter to **false**. For example, to disable the calendar service:

```
mgadmin config modify -o caldav.enable -v false
```

For more information on Mobile Synchronization Gateway service ***.enable** configuration parameters, see "Mobile Synchronization Gateway Configuration Files and Parameters".

Log Messages Indicating a Problem

If Mobile Synchronization Gateway is experiencing problems with one or more of the back-end services, examine the log files for potential issues.

For example, the following messages indicate problems with the Contacts Server back-end host:

```
Doing health check for CardDAV at http://carddav.example.com:8080/dav/principals/
<...DAVOperation.failed>  - cant reach Server at
http://carddav.example.com:8080/dav/principals/ : Connection refused
java.net.ConnectException: Connection refused
Failed health check for CardDAV at http://carddav.example.com:8080/dav/principals/
```

The same kind of log messages can appear for the Calendar Server back-end host.

Additionally, the following log messages indicate problems with the Messaging Server back-end host:

```
<...ASServer.getIMAPClient> No IMAP Client for imap.example.com - creating one
<...IMAPClientImpl$IMAPStorePool.getPROTH> failed to connect to IMAP Store:
Couldn't connect to host, port: imap.example.com, 143; timeout 60000
```

Troubleshooting Mobile Synchronization Gateway Clients

Use the information in this section to troubleshoot client issues.

iOS 7 Known Issues

This section contains iOS7 known issues.

Event Remains Canceled After Removing an Attendee from Event and Adding Back

Through Convergence, if you create an event and invite attendees to the event, then remove and add back an attendee, the event remains on the attendee's iPhone as canceled. You can then change the event time in Convergence, which does update the event time on the iPhone, however, the event remains canceled.

Unable to Create Calendar in iOS

Calendar creation fails from an iOS device when attempting to create a nested calendar. This is a bug with iOS.

A

Mobile Synchronization Gateway Command-Line Utilities

This appendix provides information about the Oracle Communications Mobile Synchronization Gateway command-line utilities.

Overview of the Command-Line Utilities

You use the mgadmin command to administer Mobile Synchronization Gateway. The **mgadmin** command is installed in the *MobileSyncGateway_home*/**sbin** directory with user or group **bin/bin** permissions.

> **Note:** The **mgadmin** command administers aspects of the server and does not affect any LDAP entries.

mgadmin Security

The **mgadmin** command requires you to authenticate with a user name and password to be able to communicate with the server. You can use the **mgadmin passfile** operation to store the necessary passwords in an encrypted *wallet* for use by subsequent **mgadmin** commands. If you do not store passwords in the wallet, then you must enter them by using a no-echo prompt on the command line. See "passfile Operation" for more information on how to create a file to store passwords.

Environment Variable

Table A–1 shows the environment variable that you can use with the various **mgadmin** commands.

Table A–1 mgadmin Environment Variable

Environment Variable	Description
MGADMIN_CLIFILE	Specifies the path to the bootstrap file. Can be used instead of the **-F** option.

mgadmin Utility

Use the **mgadmin** utility to administer Mobile Synchronization Gateway.

Location

MobileSyncGateway_home/**sbin**

General Syntax

mgadmin [*operation*] [*action*]] [*option1*] [*option2*] ...

where:

- *operation* is the **mgadmin** operation to run. See "mgadmin Operations" for more information.
- *action* is the action that the specified operation performs, such as **create**, **delete**, **list**, and **modify**. Specifying an action is optional for certain operations.
- *option* is one or more command-line options that identify information that the operation needs and the specifics of what the operation does. For example, some options provide connection parameters, and the **-o** option specifies a configuration parameter that the **config** operation can list or modify. All options are optional if the **clifile** is used and accessed through the environment variable **MGADMIN_CLIFILE**.

You can abbreviate an *operation*, an *action*, or both if they are unique in the command. For example, for the command **mgadmin config list**, you can enter **mgadmin c l**.

The default *action* for most commands is **list**. The default is used when you do not specify the *action*. For example, the following command lists the value of the **base.ldapinfo.cachesize** configuration parameter.

```
mgadmin config -o base.ldapinfo.cachesize
```

Ways to Provide Options

You can provide options to the **mgadmin** command by:

- Using the command line
- Using the **clifile**
- Including them in the **mgadmin.properties** file

Any user can create a **clifile**. Only the administrative user can use the **mgadmin.properties** file. The **mgadmin.properties** file is installed in the *MobileSyncGateway_home*/**config** directory.

When you run the **mgadmin** command, any option that you include on the command line takes precedence over the same option in the **clifile** or the **mgadmin.properties** file. Use of the **clifile** or the **mgadmin.properties** file is mutually exclusive. If you use the **clifile**, use it for any option that is not on the command line. If you run the **mgadmin** command as the administrative user and do not supply a **clifile**, the **mgadmin.properties** file is used for any option that is not on the command line.

The **mgadmin.properties** file contains values for the **userid**, **hostname**, **port**, and **secure** properties based on what you input during the initial configuration.

Clifile Properties

Table A–2 shows the properties you can specify in the bootstrap file (**clifile**):

Table A–2 Clifile Properties

Property	Description
userid	Specifies the Oracle GlassFish Administrator user ID.
usepasswordfile	Specifies whether to use the **password** file. Use **y**, **yes**, or **true** to use the password file. Use **n**, **no**, **false**, or an empty string to suppress use of the **password** file.
hostname	Specifies the GlassFish Server host name.
port	Specifies the GlassFish administration port (JMX port).
secure	Specifies the path to the truststore file used for a secure connection (HTTPS).

Common Options

Table A–3 shows the options that are common to all **mgadmin** operations.

Table A–3 Common Options

Short Option	Long Option	Description
-u	**--userid**	Required. Specifies the GlassFish Server administrator user ID.
-W	**--usepasswordfile**	Indicates to the **mgadmin** command to use the **password** file, if available.
-F	**--clifile**	Specifies the path to the file containing bootstrap information.
-H	**--hostname**	Specifies the server's host name. The default is **localhost**.
-p	**--port**	Specifies the server's administrative port number.
-s	**--secure**	Specifies the path and name of the **trustStore** file for a secure connection (HTTPS).
-h	**--help**	Displays help.
-V	**--version**	Lists the version of the **mgadmin** utility. (Checks the local package version on the disk, which can be different than what has been deployed to GlassFish Server. Version differences can occur, for example, if you added a patch but you have not yet run the **init-config** command.)

Each operation also has its own specific options, as shown in the following sections.

mgadmin Operations

Table A–4 describes the **mgadmin** operations.

Table A–4 mgadmin Operations

Operation	Description
config	Performs configuration operations, such as display the value of a particular option, set a particular option, or list all options. Some configuration operations require you to restart Mobile Synchronization Gateway. The **mgadmin config modify** command informs you if the change requires a server restart to take effect.
passfile	Creates, deletes, lists, or modifies passwords in the wallet.
version	Displays the product version. Mobile Synchronization Gateway Server is queried for its version.

Each operation takes various command-line options. Table A–3, " Common Options" describes the common options used by all **mgadmin** operations.

Note: Any option value that contains special characters or spaces must be enclosed in quotes ("") so that it is passed "as is" to the **mgadmin** command. For example:

```
mgadmin config modify -o base.ldapinfo.ugldap.binddn -v
"cn=Directory Manager"
```

---

mgadmin config

Use this command to list or modify Mobile Synchronization Gateway configuration parameters. See Appendix B, "Mobile Synchronization Gateway Configuration Files and Parameters" for the complete list of configuration parameters.

Syntax

```
mgadmin config [list|modify]
               [-u id] [-W] [-F clifile] [-H hostname]
               [-p port] [-s path] [-o property] [-v value]
               [-d] [-f file] [-e] [-q] [-h] [-M]
```

config Operation

Table A–5 describes the actions for the **config** operation.

Table A–5 Actions for config Operation

Action	Description
list	Lists all configuration settings. This is the default action if not included on the command line.
modify	Modifies a configuration setting.

At least one of the options in Table A–6 must be provided, unless you are displaying usage by using the **-h** option.

Options for config Operation

Table A–6 describes the options for the **config** operation.

Table A–6 Options for config Operation

Short Option	Long Option	Description
-o	**--option**	Specifies the configuration parameter name. Displays the configuration parameter's value if specified without the **-v** option. Sets the configuration parameter's value if specified with the **modify** action and the **-v** option.
-v	**--value**	Specifies the value that you want to set for the configuration parameter identified by the **-o** option.
-f	**--file**	Specifies the local file that contains the configuration *option=value* entries to set. Pay attention to backslashes included in this input file. Backslashes are treated as an escape character for the next character in the line. For a single backslash to be properly interpreted in a string, you must precede each backslash with another backslash. That is, use an additional backslash. For example, to include the string "aaa\bbb", you would use "**aaa\\bbb**". This is due to the way that Java reads in properties files. For more information, see the **load(Reader reader)** method of the **java.util.Properties** class at: `https://docs.oracle.com/javase/7/docs/api/`
-M	**--modonly**	Lists all of the configuration parameters that have been modified (that is, that contain nondefault values).

Table A–6 (Cont.) Options for config Operation

Short Option	Long Option	Description
-d	**--default**	Sets the value of a configuration parameter to the default when used with the **modify** action. Lists the default value when used with the **list** action.
-q	**--quiet**	Suppresses output of information messages, such as "A server restart is required."
-h	**--help**	Shows description of **config** option if specified with **-o**. Otherwise, shows the usage of **mgadmin config**.

config Examples

To show all configuration parameters:

```
mgadmin config list
(or, because list is the default option)
mgadmin config
```

To show the current setting for the error log:

```
mgadmin config -o log.mg.errors.loglevel
```

To set the error log to accept "finest" messages:

```
mgadmin config modify -o log.mg.errors.loglevel -v FINEST
```

To list the default setting of the **base.ldapinfo.authldap.ldaptimeout** parameter:

```
mgadmin config list -o base.ldapinfo.authldap.ldaptimeout -d -u admin
Enter Admin password:
base.ldapinfo.authldap.ldaptimeout: 60
```

To set the **base.ldapinfo.authldap.ldaptimeout** parameter back to its default setting:

```
mgadmin config modify -o base.ldapinfo.authldap.ldaptimeout -d -u admin
```

mgadmin passfile

Use this command to create, delete, list, or modify the **password** file for Mobile Synchronization Gateway.

When running the **mgadmin command**, instead of having to enter passwords at the no-echo prompt, you can supply passwords by using the **password** file. The **password** file is an encrypted "wallet," which holds all passwords that **mgadmin** might use. The **mgadmin passfile** operation creates, deletes, or modifies this **password** file.

Syntax

```
mgadmin passfile [ create | delete | list | modify ]
                 [-u id] [-W] [-F clifile] [-H hostname]
                 [-p port] [-s path] [-h]
```

passfile Operation

Table A–7 describes the actions for the **passfile** operation. The default action is **list**. The **passfile** operation takes no specific options.

Table A–7 Actions for passfile Operation

Action	Description
create	Creates the **password** file. If it already exists, modifies it.
delete	Deletes passwords in the **password** file. For each password, you are asked if it should be removed.
list	Displays all passwords in the **password** file.
modify	Modifies passwords in the **password** file.

passfile Examples

To modify the migration administrative password:

```
mgadmin passfile modify
Enter the Password File password:

Do you want to set the app server admin user password (y/n)? [n] y
Enter the app server admin user password:
Reenter the app server admin user password:
```

To list all the passwords:

```
mgadmin passfile list
Enter the Password File password:

The app server admin user password: password
```

mgadmin version

Use the **mgadmin version** command to display the Mobile Synchronization Gateway version. This command communicates with the server to get its version string.

Syntax

```
mgadmin version
```

version Operation

The **version** operation does not have any options.

version Example

To display the current Mobile Synchronization Gateway Server version:

```
mgadmin version
Enter Admin password:
```

B

Mobile Synchronization Gateway Configuration Files and Parameters

This appendix provides information about the Oracle Communications Mobile Synchronization Gateway configuration files and parameters.

mgserver.properties File

The **mgserver.properties** file contains the main configuration settings. It consists of configuration parameters and their current values.

> **Caution:** Do not edit this file by hand. Always use the **mgadmin** command to set configuration parameters.

The format of the **mgserver.properties** file is:

```
parameter=value
parameter=value
:
:
```

mgservercreds.properties File

The **mgservercreds.properties** file contains the password configuration settings. It consists of configuration parameters that are passwords and their current values.

> **Caution:** Do not edit this file by hand. Always use the **mgadmin** command to set configuration parameters.

The format of the **mgservercreds.properties** file is:

```
password_parameter=value
password_parameter=value
:
:
```

mgadmin.properties File

You can provide options to the **mgadmin** command by including them in the **mgadmin.properties** file.

Table B–1 describes the parameters in the **mgadmin.properties** file.

Table B–1 mgadmin.properties File Parameters

Parameter	Description
userid	Specifies the Oracle GlassFish Administrator user ID.
hostname	Specifies the GlassFish Server host name.
port	Specifies the GlassFish administration port (JMX connector port).
secure	Specifies the path to the truststore file used for a secure connection (HTTPS) to Glassfish Server.
sslprotocols	Specifies the supported SSL protocols (**TLSv1**, **TLSv1.1**, and **TLSv1.2**) for the JMX proxy to communicate with management beans in the server.

The format of the **mgadmin.properties** file is:

```
parameter=value
parameter=value
:
:
```

Mobile Synchronization Gateway Configuration Parameters

Table B–2 lists the configuration parameters and descriptions for Mobile Synchronization Gateway. See "Mobile Synchronization Gateway Command-Line Utilities" for information about updating or changing configuration parameters by using the **mgadmin config modify** command.

Table B–2 Mobile Synchronization Gateway Configuration Parameters

Parameter	Type	Description	Default value
base.ldapinfo.cachesize	integer	Size of the LDAP Authentication cache.	**1000**
base.ldapinfo.cachettl	integer (seconds)	Time to live (in seconds) of cached LDAP Authentication info.	**60**
base.ldapinfo.dcroot	string	Root of DC tree (Schema 1) or of the domain and users tree (Schema 2) in Directory Server	Value derived from **comm_dssetup.pl** script.
base.ldapinfo.defaultdomain	string	Default domain.	Value derived from **comm_dssetup.pl** script.
base.ldapinfo.domainattrs	string	Space separated list of LDAP attributes to use when retrieving domain information.	**externalAuthPreUrlTemplate externalAuthPostUrlTemplate** **mgStatus**
base.ldapinfo.loginseparator	string	Characters to be used as login separator (between userid and domain).	**@**

Table B–2 (Cont.) Mobile Synchronization Gateway Configuration Parameters

Parameter	Type	Description	Default value
base.ldapinfo.schemalevel	integer	Specifies the schema level.	Value derived from **comm_dssetup.pl** script.
base.ldapinfo.searchfilter	string	Specifies the search filter for looking up users during authentication when one is not specified in the **inetDomainSearchFilter** for the domain. The syntax is the same as **inetDomainSearchFilter**. For more information, see *Communications Suite Schema Reference*.	**(|(uid=%U)(mail=%o))**
base.ldapinfo.serviceadmindn	string	DN of single administrator in LDAP in absence of administrative group.	None
base.ldapinfo.serviceadminsgroupdn	string	DN of service administrators group in LDAP.	**cn=Service Administrators,ou=Groups,***UGSuffix*
base.ldapinfo.authldap.binddn	string	Distinguished Name to use when authenticating.	None
base.ldapinfo.authldap.bindpassword	password	Password to use when authenticating.	None
base.ldapinfo.authldap.ldaphost	string	Space-delimited list of host names. Each host name can include a trailing colon and port number.	None
base.ldapinfo.authldap.ldappoolrefreshinterval	integer (minutes)	Length of elapsed time until the failover Directory Server host reverts back to the primary Directory Server host. If set to **-1**, do not refresh the interval.	**1**
base.ldapinfo.authldap.ldappoolsize	integer	Maximum number of connections for this pool.	**10**
base.ldapinfo.authldap.ldapport	integer	Directory Server host port number to which to connect. Ignored for any host name that includes a colon and port number.	**389**
base.ldapinfo.authldap.ldaptimeout	integer (seconds)	Timeout for all LDAP operations.	**60**
base.ldapinfo.authldap.ldapusessl	boolean	Use SSL to connect to the LDAP host.	**false**

Table B–2 (Cont.) Mobile Synchronization Gateway Configuration Parameters

Parameter	Type	Description	Default value
base.ldapinfo.authldap.sslprotocols	string	Specifies a space-delimited list of the supported SSL protocols to communicate with the back-end LDAP service.	**TLSv1 TLSv1.1 TLSv1.2**
base.ldapinfo.userattrs	string	Space separated list of LDAP attributes to retrieve from user entries during the authentication phase.	**mail ismemberof**
base.ldapinfo.ugldap.binddn	string	Distinguished Name to use when authenticating.	**cn=Directory Manager**
base.ldapinfo.ugldap.bindpassword	password	Password to use when authenticating.	None
base.ldapinfo.ugldap.ldaphost	string	Space-delimited list of host names. Each host name may include a trailing colon and port number.	**localhost:389**
base.ldapinfo.ugldap.ldappoolrefreshinterval	integer (minutes)	Length of elapsed time until the failover Directory Server host reverts back to the primary Directory Server host. If set to **-1**, do not refresh the interval.	**1**
base.ldapinfo.ugldap.ldappoolsize	integer	Maximum number of connections for this pool.	**10**
base.ldapinfo.ugldap.ldapport	integer	Port number to which to connect. Ignored for any host name that includes a colon and port number.	**389**
base.ldapinfo.ugldap.ldaptimeout	integer (seconds)	Timeout for all LDAP operations.	**60**
base.ldapinfo.ugldap.ldapusessl	boolean	Use SSL to connect to the LDAP host.	**false**
base.ldapinfo.ugldap.sslprotocols	string	Specifies a space-delimited list of the supported SSL protocols to communicate with the back-end LDAP service.	**TLSv1 TLSv1.1 TLSv1.2**
base.ldappool.*.binddn	string	Distinguished Name to use when authenticating.	None, specified during LDAP pool creation
base.ldappool.*.bindpassword	password	Password to use when authenticating.	None, specified during LDAP pool creation

Table B–2 (Cont.) Mobile Synchronization Gateway Configuration Parameters

Parameter	Type	Description	Default value
base.ldappool.*.ldaphost	string	Space-delimited list of host names. Each host name may include a trailing colon and port number.	**localhost:389**
base.ldappool.*.ldappoolrefreshinterval	integer (minutes)	Length of elapsed time until the failover Directory Server host reverts back to the primary Directory Server host. If set to **-1**, do not refresh the interval.	**1**
base.ldappool.*.ldappoolsize	integer	Maximum number of connections for this pool.	**10**
base.ldappool.*.ldapport	integer	Port number to which to connect. Ignored for any host name which includes a colon and port number.	**389**
base.ldappool.*.ldaptimeout	integer (seconds)	Timeout for all LDAP operations.	**60**
base.ldappool.*.ldapusessl	boolean	Use SSL to connect to the LDAP host.	**false**
base.ldappool.*.sslprotocols	string	Specifies a space-delimited list of the supported SSL protocols for the LDAP pool to communicate with the back-end LDAP service.	**TLSv1 TLSv1.1 TLSv1.2**
caldav.enable	boolean	Specifies whether the calendar service is enabled or not.	**true**
caldav.enablessl	boolean	Use SSL to connect to the server.	**true**
caldav.host	string	FQDN host name of the Oracle Communications Calendar Server host.	None
caldav.httppoolsize	integer	Maximum number of connections established to this host.	**50**
caldav.mqhosturls	string	URL list of Calendar Server hosts on which Message Queue is running, separated by a comma. URL is in the form of *host*:*port*, for example: **sc111.example.com,localhost:7676**	None

Table B–2 (Cont.) Mobile Synchronization Gateway Configuration Parameters

Parameter	Type	Description	Default value
caldav.mqport	integer	Java Messaging Service port on the Calendar Server host to which to connect	**7676**
caldav.port	integer	Calendar Server port number to which to connect.	**443**
caldav.proxyadminid	string	The Calendar Server proxy administrative UID. This should be in the form: *uid@domain* if hosted domains setup is used.	**calmaster**
caldav.proxyadminpassword	password	The Calendar Server proxy administrative password.	None
caldav.requesttimeout	integer (seconds)	The time in seconds to wait for the Calendar Server host to respond before timing out.	**60**
caldav.serviceuri	string	Context path at which the DAV interface is accessible.	**/dav**
caldav.sslprotocols	string	Specifies a space-delimited list of the supported SSL protocols to communicate with the back-end Calendar Server service.	**TLSv1 TLSv1.1 TLSv1.2**
carddav.enable	boolean	Enables CardDAV protocol.	**true**
carddav.enablessl	boolean	Use SSL to connect to the Oracle Communications Contacts Server host.	**true**
carddav.host	string	FQDN host name of the Contacts Server host.	**localhost**
carddav.httppoolsize	integer	Maximum number of connections established to this Contacts Server host.	**50**
carddav.mqhosturls	string	URL list of Contacts Server hosts on which Message Queue is running, separated by a comma. URL is in the form of *host***:***port*, for example: **cs111.example.com,localhost:7676**	None

Table B–2 (Cont.) Mobile Synchronization Gateway Configuration Parameters

Parameter	Type	Description	Default value
carddav.mqport	integer	Java Message Service port on the Contacts Server host to which to connect.	**7676**
carddav.port	integer	Contacts Server port number to which to connect.	**443**
carddav.proxyadminid	string	The Contact Server proxy administrative UID. This should be in the form: *uid@domain* if hosted domains setup is used.	**nabmaster**
carddav.proxyadminpassword	password	The Contacts Server proxy administrative password.	None
carddav.requesttimeout	integer (seconds)	The time in seconds to wait for the Contacts Server host to respond before timing out.	**60**
carddav.serviceuri	string	Context path at which the CardDAV interface is accessible.	**/dav**
cardav.sslprotocols	string	Specifies a space-delimited list of the supported SSL protocols to communicate with the back-end Contacts Server service.	**TLSv1 TLSv1.1 TLSv1.2**
imap.enablessl	boolean	Use SSL to connect to the Oracle Communications Messaging Server host.	**true**
imap.host	string	FQDN host name of the default IMAP server. Other IMAP servers are discovered through the **mailhost** LDAP attribute.	None
imap.inactivitytimeout	integer (seconds)	Time value in seconds after which unused connections are closed. One connection remains active.	**300**
imap.port	integer	IMAP server port number to which to connect.	**993**
imap.proxyadminid	string	IMAP server's proxy administrative UID. This should be of the form *uid@domain* if you use hosted domains.	**admin**

Table B–2 (Cont.) Mobile Synchronization Gateway Configuration Parameters

Parameter	Type	Description	Default value
imap.proxyadminpassword	password	IMAP server's proxy administrative password.	None
imap.requesttimeout	integer (seconds)	The time in seconds to wait for the IMAP server to respond before timing out.	**60**
imap.sslprotocols	string	Specifies a space-delimited list of the supported SSL protocols to communicate with the back-end IMAP service.	**TLSv1 TLSv1.1 TLSv1.2**
iwc.host	string	FQDN host name of the default Oracle Communications Convergence server.	None
iwc.port	integer	Convergence server port number to which to connect.	**443**
iwc.enablessl	boolean	Use SSL to connect to the Convergence host.	**true**
iwc.serviceuri	string	Context path at which the Convergence interface is accessible.	**/iwc/svc/iwcp**
iwc.proxyadminid	string	Convergence server's proxy administrative UID. This should be of form *uid@domain* if you use hosted domains.	**admin**
iwc.proxyadminpassword	password	Convergence server's proxy administrative password.	None
iwc.requesttimeout	integer (seconds)	The time in seconds to wait for the Convergence server to respond before timing out.	**60**
iwc.httppoolsize	integer	Maximum number of connections established to this Convergence server.	**50**
iwc.sslprotocols	string	Specifies a space-delimited list of the supported SSL protocols to communicate with the back-end Convergence service.	**TLSv1 TLSv1.1 TLSv1.2**
log.mg.commands.logdateformat	logdateformat	Specifies the date format pattern for the log.	*yyyy-MM-dd*'**T**'*HH*:*mm*:*ss.SSSZ*

Table B–2 (Cont.) Mobile Synchronization Gateway Configuration Parameters

Parameter	Type	Description	Default value
log.mg.commands.logdir	filepath	Directory path for log files.	**logs**
log.mg.commands.loglevel	loglevel	Specifies the log level. Valid levels are **OFF** (no information is logged), **SEVERE**, **WARNING**, **INFO**, **CONFIG**, **FINE**, **FINER**, **FINEST**, and **ALL** (all information is logged). The **FINEST** and **ALL** levels produce a large amount of data.	**INFO**
log.mg.commands.logtoparent	boolean	Enables logging to the GlassFish Server log file, in addition to the Mobile Synchronization Gateway logs.	**false**
log.mg.commands.maxlogfiles	integer	Maximum number of log files.	**10**
log.mg.commands.maxlogfilesize	integer (bytes)	Maximum size of each log file.	**2097152**
log.mg.errors.logdateformat	logdateformat	Specifies the date format pattern for the log.	*yyyy-MM-dd***'T'***HH*:*mm*:*ss.SSSZ*
log.mg.errors.logdir	filepath	Directory path for log files.	**logs**
log.mg.errors.loglevel	loglevel	Specifies the log level. Valid levels are **OFF** (no information is logged), **SEVERE**, **WARNING**, **INFO**, **CONFIG**, **FINE**, **FINER**, **FINEST**, and **ALL** (all information is logged). The **FINEST** and **ALL** levels produce a large amount of data.	**INFO**
log.mg.errors.logtoparent	boolean	Enables logging to the GlassFish Server log file, in addition to the Mobile Synchronization Gateway logs.	**false**
log.mg.errors.maxlogfiles	integer	Maximum number of log files.	**10**
log.mg.errors.maxlogfilesize	integer (bytes)	Maximum size of each log file.	**2097152**
log.mg.telemetry.logdateformat	logdateformat	Specifies the date format pattern for the log.	*yyyy-MM-dd***'T'***HH*:*mm*:*ss.SSSZ*

Table B–2 (Cont.) Mobile Synchronization Gateway Configuration Parameters

Parameter	Type	Description	Default value
log.mg.telemetry.logdir	filepath	Directory path for log files.	**logs**
log.mg.telemetry.loglevel	loglevel	Specifies the log level. Valid levels are **OFF** (no information is logged), **SEVERE**, **WARNING**, **INFO**, **CONFIG**, **FINE**, **FINER**, **FINEST**, and **ALL** (all information is logged). The **FINEST** and **ALL** levels produce a large amount of data.	**INFO**
log.mg.telemetry.logtoparent	boolean	Enables logging to the GlassFish Server log file, in addition to the Mobile Synchronization Gateway logs.	**false**
log.mg.telemetry.maxlogfiles	integer	Maximum number of log files.	**10**
log.mg.telemetry.maxlogfilesize	integer (bytes)	Maximum size of each log file.	**2097152**
mail.autoreply.autoreplysubject	string	Subject for out of office email replies.	**Out of office**
mail.autoreply.autoreplytimeout	integer	Determines how often (in hours) users receive an out of office reminder. Values can be a positive integer between 1 and 300.	**168**
mgcore.auth.cert.enable	boolean	Enables certificate-based client authentication.	**false**
mgcore.auth.cert.fallback	boolean	Enables fallback to username and password authentication.	**true**
mgcore.ldapattr.carddavuserattr	string	LDAP attribute whose presence in a user LDAP entry identifies a CardDAV user. This attribute is used only when both CardDAV and WABP address book protocols are configured.	**nabStore**
mgcore.ldapattr.commonname	string	Specifies the common name attribute.	**cn**

Table B–2 (Cont.) Mobile Synchronization Gateway Configuration Parameters

Parameter	Type	Description	Default value
mgcore.ldapattr.externalauthposturltemplate	string	LDAP attribute that determines whether external authentication should do a post-authentication lookup against this domain.	**externalAuthPostUrlTemplate**
mgcore.ldapattr.externalauthpreurltemplate	string	LDAP attribute that determines whether external authentication is used against this domain.	**externalAuthPreUrlTemplate**
mgcore.ldapattr.inetuserstatus	string	LDAP attribute for status of user's account with regards to global service access.	**inetuserstatus**
mgcore.ldapattr.mail	string	Specifies the mail attribute.	**mail**
mgcore.ldapattr.mailalternateaddress	string	Separated list of alternate mail attributes.	**mailAlternateAddress**
mgcore.ldapattr.mailhost	string	Specifies the mail host attribute.	**mailhost**
mgcore.ldapattr.memberattr	string	LDAP attribute listing the groups of which the entry is a member.	**ismemberof**
mgcore.ldapattr.preferredlang	string	Language attribute.	**preferredLanguage**
mgcore.ldapattr.status	string	Mobile Synchronization Gateway status attribute that sets if service is active, inactive, deleted, or removed.	**mgStatus**
mgcore.ldapattr.uid	string	User ID attribute.	**uid**
mgcore.ldapsubject.emailsearchfiltertemplate	string	LDAP filter used when searching a subject by email address. The %s tokens are replaced by the email value to search.	**|(mail=%s)(mailalternateaddress=%s)**

Table B–2 (Cont.) Mobile Synchronization Gateway Configuration Parameters

Parameter	Type	Description	Default value
mgcore.ldapsubject.ldapcachesize	integer	Maximum number of subjects (LDAP users, resources, and groups) kept in cache when mapping email and subjects. Entries are removed from the cache only when this maximum is reached or when any of the **ldap subject** configuration parameters are changed. Can be set to **0**, indicating no cache.	**1000**
mgcore.ldapsubject.ldapcachettl	integer (seconds)	Maximum time (in seconds) that subjects (LDAP users) are kept in cache when mapping emails and subjects.	**60**
mgcore.ldapsubject.subjectattributes	string	Space separated list of LDAP attribute names to retrieve when doing a search for users.	**cn mgstatus mail mailalternateaddress preferredlanguage uid objectclass mailhost nabStore**
mgcore.serverdefaults.sslprotocols	string	Specifies a space-delimited list of the supported SSL protocols as the default for the various back-end services' **sslprotocols** configuration. That is, if the specific **sslprotocols** parameter is not set, it is set to the value of **mgcore.serverdefaults .sslprotocols**.	**TLSv1 TLSv1.1 TLSv1.2**
mgcore.telemetry.filter	string	Space separated list of email addresses of users to be logged by telemetry.	**ALL**
mgcore.telemetry.forcetelemetry	boolean	Force telemetry for all users. Use caution when enabling as it generates a lot of data.	**false**

Table B–2 (Cont.) Mobile Synchronization Gateway Configuration Parameters

Parameter	Type	Description	Default value
service.as.autodiscover.autodiscovername	string	Name element of the Server element in Autodiscover command responses from the EAS server. The Name element is an optional child element of the Server element in Autodiscover command responses that specifies the URL. If the **Type** element value is **MobileSync**, then the **Name** element specifies the URL that conveys the protocol.	**http://***localhost*
service.as.autodiscover.autodiscoverurl	string	URL element in Autodiscover command responses from the EAS Server. The URL element is an optional child element of the **Server** element in Autodiscover command responses that specifies a URL that conveys the protocol, port, resource location and other information.	**http://***localhost*
service.as.heartbeat.maxheartbeatinterval	integer	Maximum acceptable heartbeat interval.	**3540**
service.as.heartbeat.minheartbeatinterval	integer	Minimum acceptable heartbeat interval.	**60**
service.as.heartbeat.pollingheartbeatinterval	integer	Polling heartbeat interval (used when push is not enabled). Clients are awoken after this interval, with a status indicating that changes have occurred. A value of zero indicates that polling is disabled.	**0**

Table B–2 (Cont.) Mobile Synchronization Gateway Configuration Parameters

Parameter	Type	Description	Default value
service.as.monitor.enable	boolean	Enables the Mobile Synchronization Gateway monitoring service. You do not need to restart Mobile Synchronization Gateway for response time metrics. You do need to restart Mobile Synchronization Gateway for back-end connection status and data collection interval change.	**true**
service.as.monitor.probeinterval	integer	Specifies the interval, in seconds, of the monitoring service's data collection frequency, within the range of 60 to 3600. You must restart Mobile Synchronization Gateway for an interval change to take effect.	**300**
service.as.push.mqpswd	password	Java Message Queue user password.	**guest**
service.as.push.mquser	string	Java Message Queue user name.	**guest**
service.as.push.port	integer	Specifies the port number of a message broker instance.	**7997**
smtp.enablessl	boolean	Use SSL to connect to the SMTP server.	**false**
smtp.host	string	FQDN host name of the SMTP host.	**localhost**
smtp.inactivitytimeout	integer (seconds)	Time value in seconds after which unused connections are closed.	**300**
smtp.port	integer	Port number to use to connect to the SMTP host.	**25**
smtp.proxyadminid	string	SMTP server's proxy administrative UID. This should be of the form *uid@domain* if you use hosted domains.	None
smtp.proxyadminpassword	password	SMTP server's proxy administrative password.	None

Table B–2 (Cont.) Mobile Synchronization Gateway Configuration Parameters

Parameter	Type	Description	Default value
smtp.requesttimeout	integer (seconds)	Time in seconds to wait for the SMTP server to respond before timing out.	**30**
smtp.sslprotocols	string	Specifies a space-delimited list of the supported SSL protocols to communicate with the back-end SMTP service.	**TLSv1 TLSv1.1 TLSv1.2**
wabp.enablessl	boolean	Use SSL to connect to the Convergence server that provides WABP information.	**true**
wabp.host	string	FQDN host name of the Convergence server that provides WABP information.	None
wabp.httppoolsize	integer	Maximum number of connections established to this Convergence server that provides WABP information.	**50**
wabp.port	integer	Port number to which to connect to the Convergence server that provides WABP information.	**443**
wabp.proxyadminid	string	Proxy administrative UID of the Convergence server that provides WABP information. This should be of the form *uid@domain* if you use hosted domains.	**admin**
wabp.proxyadminpassword	password	Proxy administrative password of the Convergence server that provides WABP information.	None

Table B–2 (Cont.) Mobile Synchronization Gateway Configuration Parameters

Parameter	Type	Description	Default value
wabp.requesttimeout	integer (seconds)	Time in seconds to wait for the Convergence server that provides WABP information to respond before timing out.	**60**
wabp.serviceuri	string	Context path at which the WABP interface is accessible.	**/iwc/svc/wabp**
wabp.sslprotocols	string	Specifies a space-delimited list of the supported SSL protocols to communicate with the back-end WABP service.	**TLSv1 TLSv1.1 TLSv1.2**