

# Managing Devices Remotely With Oracle Database Lite

*An Oracle White Paper  
August 2007*

# Managing Devices Remotely With Oracle Database Lite

## Table of Contents

Overview.....	3
Device Management Architecture .....	3
How you can Manage Your Mobile Devices .....	5
Automatically Update Software on Mobile Client .....	5
Controlled Updates for Multiple Users.....	5
Remote Command Execution .....	6
Creating a Group Command.....	8
Scheduling Commands .....	9
Enabling or Disabling All Mobile Devices in a Platform .....	9
Viewing Device Management On the Client.....	9
Enable Pull Option .....	10
Retry Count.....	10
Check for Update.....	10
Proxy Server.....	10
Create Your Own Device Commands .....	10
Device Management Security .....	11
Configure Device Management to Work With a Firewall.....	11

# Managing Devices Remotely With Oracle Database Lite

## OVERVIEW

Since the mobile device environment is exploding, administrators are managing enterprises with hundreds—and sometimes thousands—of distributed devices. This creates the question of how to manage modifications for the devices—whether it is software updates, changing users who own the device or modifying the database schema for the application.

The following are questions that concern administrators who support multiple remote workers:

- How do I manage every worker's device to handle changes in the database table schema, application modifications, and software updates?
- How can I track and review what exists and who owns each mobile device in the enterprise?

Oracle Database Lite solves these questions with a device management agent installed on the Mobile client that enables the administrator to remotely track, update, and manage the device software and configuration. When you install the Oracle Database Lite Mobile client software, the Device Manager agent is also installed. The Device Manager enables the administrator to manage the company's devices remotely. With the Device Manager agent installed and enabled, the administrator can send commands to remote devices for gathering information, upgrading or installing software, or disabling or uninstalling the client. You can use the Device Manager agent for most administrative actions between the Mobile Server and the Mobile client.

In addition, the Mobile client or the application can use the Device Manager agent to perform device management locally.

## DEVICE MANAGEMENT ARCHITECTURE

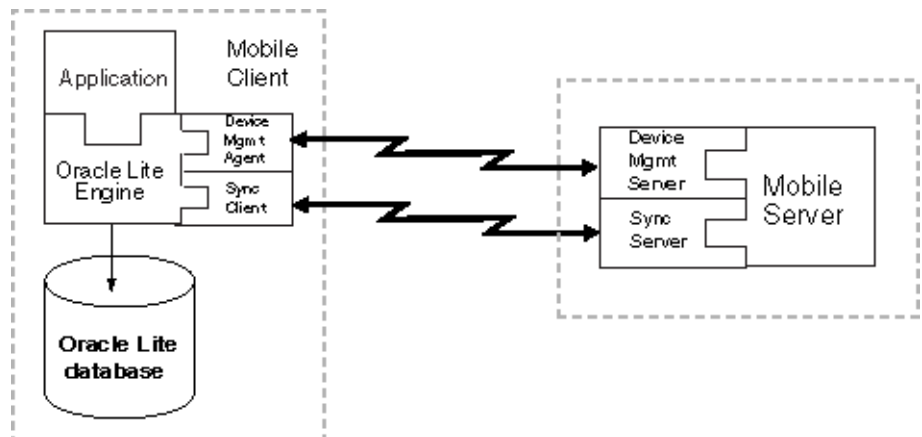
When you install your Mobile client software, the Mobile device manager client software is automatically installed and bootstrapped. Once the device is bootstrapped, then the administrator can send commands from Mobile Manager to one or more remote devices. The next time that the device is available—either

through wireless connection or synchronization—the command that is sent executes on the device.

Device management is facilitated between the Mobile client and the Mobile Server with the following components:

- The Device Management agent on the client receives and executes incoming requests from the Mobile Server. The agent—also known as `dmagent`—is installed on the client when the Mobile client is installed. It works in conjunction with the Oracle Database Lite engine to perform the tasks either assigned locally by the user or application or requested remotely from the Mobile Server by an administrator.
- The Device Management Server is installed with the Mobile Server. Its responsibilities are to forward all commands from the Mobile Server to the Device Management Agent on the client and to receive all responses from this agent.

The following graphic displays the architecture of the Device Management agent within the Mobile client. It shows how the administrator can send commands to the agent remotely from the Mobile Server and that the device management uses a separate communications line than the synchronization management.



The Device Management System operates using an asynchronous command/response protocol, as follows:

1. The Device Management Server (DMS) on the Mobile Server sends device specific commands to the Device Management Agent (DMA) on the client.
2. The DMA processes the commands on the client and sends all results back to the DMS on the Mobile Server.

DMS sends commands over one of the Network Providers defined by the administrator, which could be HTTP, RAPI or SMS/Wake-on-Ring. A customer may use another messaging mechanism, if they implement it themselves and register it with DMS.

## HOW YOU CAN MANAGE YOUR MOBILE DEVICES

The following sections describe how you, as an administrator, can manage each device assigned to a user.

### Automatically Update Software on Mobile Client

You can control whether a new version of the application software is downloaded on each client and which users receive the latest update. The default configuration is for all devices attached to a user to receive current updates.

For example, you have two users: John and Tom. You want John's devices to stay at the current version, which is Oracle Database Lite Win32 version 10.0.0.0.0; however, you want Tom's devices to upgrade to the new version, which is Oracle Database Lite Win32 version 10.1.0.0.0. Configure each user's devices, as follows:

- For John, configure the update policy to Minor.
- For Tom, configure the update policy to Major.

The administrator can configure each mobile device to automatically receive new software updates when each comes available—either for the Mobile client software or for any applications installed on the client, as follows:

- All updates—Include major and minor updates.
- Major—The devices attached to this user receives only major software updates, which is denoted by the version number. Any modification of the version in the first or second position is a major update. For example, any version that changes from 10.0.0 to 10.1.0 or 11.0 is a major update. This is the default.
- Minor—The devices attached to this user receives only minor software updates. This includes only patch releases. For example, if the client software is version 10.0.0, then modifications only apply to the third position or later constitutes a patch update. This would include the version numbers 10.0.1 or 10.0.0.1. It would not include the 10.1.0 which would be a major update.
- Disable updates—The devices attached to this user does not receive any software updates.

The Device Manager invokes the update executable after synchronization completes to determine if any mobile application updates are available, then downloads and installs these application updates to a Mobile client. Alternatively, the Install Application command can be sent to the client to force an update.

### Controlled Updates for Multiple Users

If you want to roll out software updates in a staggered fashion to a subset of your users at a time, you can use the controlled update. A controlled update enables the following:

- You can deploy the latest software or patches to a set of users to limit the impact of your IT team handling multiple responses from affected users.

- You can deploy the latest software or patches to a set of users for testing purposes, while keeping the majority of the users on an older version of the software.

To perform a controlled update, perform the following within Mobile Manager:

1. Create a group with all of the users that you want to receive the update.
2. Edit the group and set the update policy for the group to All, Major, Minor or Disable.

Alternatively, you can use the APIs and perform the following:

1. Create a group with the `MobileResourceManager.createGroup` method.
2. Set the group update policy with the following method, where the value can be “major,” “minor,” or “false.”

```
group.setPolicy(ResourceConst.UPDATE_SOFTWARE, "major");
```

3. Add all users to be within the group with the `MobileResourceManager.addUsersToGroup` method.

## Remote Command Execution

Oracle Database Lite provides administrators the means to send commands remotely to mobile devices based upon users, applications or groups. The administrator can send commands to Mobile devices to inspect or modify what is currently installed or configured, start synchronization, validate the database, install and upgrade software, as well as deactivate a unit if the user is no longer allowed to access the database or if the device was lost.

These commands capture data and logs from the client or instruct the client to carry out necessary tasks. For example, the Mobile Manager could send a command to a client to perform synchronization or to remove the entire client data store, if a device may have been compromised. The next time that the device is available—either through wireless connection or synchronization—the command that you send executes on the mobile device.

The following sections describe what you can do with the commands you can send to the device.

### ***Reset Password***

If a user has forgotten their password, use this command to remotely reset the password on the device.

### ***Modify Configuration***

Modify configuration settings in the client-side POLITE.INI or ODBC.INI configuration files.

### ***Synchronization Commands***

The following commands either starts synchronization or retrieves information about a previously executed synchronization:

- Retrieve synchronization log—If the administrator needs to understand why a synchronization may not be successful for a certain device, then he/she can retrieve the data synchronization log from the client. The retrieved information can be viewed in the Mobile Manager.
- Synchronize databases—If, for some reason, the administrator needs all updates in the server at a certain time, then the administrator can issue this command to synchronize all the Mobile client databases that are able to be synchronized. For example, the administrator may want all available updates to be applied before the weekly backup.
- Synchronize and delete databases—If a mobile device has been lost or stolen, then the administrator may need to retrieve the last updates from a mobile device and then delete all databases from that device.

### ***Update Device Manager Client***

This command forces the device manager client to perform an update of the device's OTL script files with the script files located in the Mobile Server's script directory.

### ***Retrieve and View Device Information***

You can retrieve and view device information, such as the following:

- Device information, such as the following:
  - ❑ What user currently owns and uses the Mobile device.
  - ❑ The operating system, its version and the latest service pack applied. In addition, you can view the host name and last known IP address for the Mobile device.
  - ❑ How much memory you have on the device, which includes how much virtual or physical memory is on the device, and how much of that memory is still available.
  - ❑ The type of device and processor. Organizations may have rolled out several types of devices over the lifetime of a mobile deployment. With this functionality, you can determine exactly which users require device upgrades.
  - ❑ For Windows-based devices only, the version of the JDK that you have installed and where it is installed. You no longer have to ask your users to check which version of JDK that they have installed. In addition, this section describes the CLASSPATH for the Mobile client environment.

- ❑ The amount of storage space that exists and is currently available on each drive.
- Database information for the Oracle Lite database that is installed on the Mobile client, such as the following:
  - ❑ The ODBC driver name and full path to the DLL implementing the driver, so that you can know which version that is installed on your client.
  - ❑ The user client databases for each application.
  - ❑ The exact contents of the Mobile client POLITE.INI configuration file.
- Installed Oracle Database Lite software on the Mobile device, which lists each application, its version, setup time, and location details.

#### ***Retrieve a file from the device***

This command forces the device to upload a designated file, which enables the administrator to see any configuration file on the device. This can be particularly useful in diagnosing problems with the device.

#### ***Install Application***

If you need the device to install a new application, then this command forces the device to install an application. If the application already is installed on the client and an update is available, this command forces an update for the client.

#### ***Manage the Oracle Lite Database***

- Validate Database—Validates the client database and uploads the results to the Mobile Server.
- De-install Oracle Database Lite—If the device is lost or stolen, then the administrator can de-install the Oracle Database Lite client remotely. This also may be useful if it is easier to de-install the previous and install a new version of Oracle Database Lite, rather than upgrade.

### **Creating a Group Command**

You can create a group command, which is a set of existing commands that you want to execute together. The advantage is that you do not have to issue each command separately, but can combine for efficiency.

To control the order in which the commands are executed, you specify a weight for each command within the group. Users must specify a weight for all the commands within the chosen group command.

Normally, the administrator manually sends the commands after the device is up. However, to simplify the initialization process, you can specify that a group command automatically executes once the device is bootstrapped. When you

extend the platform, choose a Bootstrap group command from the list displayed. Then, choose a group command to execute when it is completed. For example, choosing the device information command retrieves all of the device information to the Mobile Manager for viewing.

### **Scheduling Commands**

You can schedule that a command executes now to a single device or to all devices within a platform. Alternatively, you can schedule any command or group command to execute at a future time within the Command Scheduler section of the Mobile Manager.

### **Enabling or Disabling All Mobile Devices in a Platform**

You can enable or disable all Mobile devices in a platform. By default, each device in the platform is enabled, which means that the user can synchronize to the database and perform software updates. If you disable the device, then it can no longer perform work for the user. You can even disable a single device—because a user has lost the device or left the company.

Why would you want to disable all devices in the platform? What if you had created a customized platform for devices that were used for a specific purpose, such as if you had mobile phones that were analog only. When you came out with a full digital network, you may not want any of the analog technology to continue to be used. You could choose to send a uninstall command and then disable all of the analog Mobile devices. Since all of them had the same platform, all of them could be disabled at the same time. The user could no longer log in and use the device. They would be forced to upgrade to digital.

### **VIEWING DEVICE MANAGEMENT ON THE CLIENT**

On any client, the user can view status and manage the Mobile device client software and commands sent to the device with the Device Manager Agent (`dmagent`). Use the Device Manager Agent for viewing information about your device, such as the version, the commands, retry count and so on.

To bring up the Device Manager GUI, choose Oracle Database Lite Device Manager from the Oracle Database Lite Programs list or you can execute `dmagent`.

The main screen provides information about the following: platform type, language, Oracle Database Lite version, device user, device name, and the URL of where the device is installed.

The options page enables you to choose whether to check for updates automatically and at what time, whether to pull down commands, and the proxy server, as follows:

### **Enable Pull Option**

If the server cannot connect to the client, any commands sent to the client are placed into the Device Manager command queue. These commands are sent to the client when one of two things occurs:

- The client synchronizes.
- A "Pull" is initiated from the client.

When you check the Enable Pull checkbox on the Device Manager agent, the device manager client automatically polls the Device command queue for any commands for this user. You can also configure the frequency—which is the number of seconds to wait between each pull.

### **Retry Count**

You can set a retry count to specify the number of times that a command is executed, if it fails to execute. If it still fails after retrying, the command is deleted. This count also applies to failed synchronization attempts. The commands are retried with the same frequency interval that is set for the Enable Pull command. A command can fail to execute if there is an error within the command or if there is no connection between the client and the server.

### **Check for Update**

Select the day and time that you want a command queued for the device manager client to automatically poll for updates. However, updates are always automatically polled for during any synchronization. Thus, this option is useful if you never synchronize with the Mobile Server.

Even though you are setting a specific time, the actual time depends on when the device manager checks for queued commands.

### **Proxy Server**

If you have a proxy server between the Mobile client and Mobile Server, you can configure the address and port for that proxy server in the Device Manager.

## **CREATE YOUR OWN DEVICE COMMANDS**

You can create your own device commands with a scripting language supplied by Oracle Database Lite called Oracle Tag Language (OTL). Combine the OTL scripting language with the Device Manager APIs to create your own specific commands. Once you create the command, load it into the Mobile Server from the Mobile Manager Create Command page.

You can customize the management of devices through gathering information on devices, sending commands to devices, registering devices, and so on. The main Device Manager API that you will use is the `oracle.lite.resource.DeviceManager` class.

## DEVICE MANAGEMENT SECURITY

The device management commands are powerful and provide an administrator a great deal of control over the mobile device population. It is important that malicious users cannot send potentially harmful commands to a user's device. Oracle Database Lite uses state of the art public/private key encryption algorithms to protect the data and authentication to verify the originator and the integrity of the commands.

## CONFIGURE DEVICE MANAGEMENT TO WORK WITH A FIREWALL

We use device management to send commands to devices for updates, initiating synchronization, and so on. Device management can be configured to use HTTP, RAPI or SMS/Wake-on-Ring as the communication protocol.

There are two types of device management requests:

- Device initiated: The device management agent (`dmagent`) that is included on the Mobile device registers with the Mobile Server at device bootstrap. The `dmagent` periodically polls the Mobile server for command requests on the Mobile Server listening port.
- Mobile Server initiated: The Mobile Server sends the commands directly to the Mobile device. You can send commands to one or more devices through the Mobile Manager or Java APIs. However, this is unusual, since most communication/synchronization is initiated from the client. Thus, the proxy must be configured correctly to enable communication initiated from the Mobile Server.

When using a firewall, then both the Mobile Server and the devices need to be configured for proxy or reverse proxy to reach each other, as follows:

- The `dmagent` on the Mobile device should be able to access the `SERVER_PORT` on the firewall.
- The Mobile Server should be able to access the `PUSH_PORT` of all devices.



Managing Devices Remotely With Oracle Database Lite  
August 2007

Oracle Corporation  
World Headquarters  
500 Oracle Parkway  
Redwood Shores, CA 94065  
U.S.A.

Worldwide Inquiries:  
Phone: +1.650.506.7000  
Fax: +1.650.506.7200  
[oracle.com](http://oracle.com)

Copyright © 2007, Oracle. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice.

This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission. Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.