webMethods Mobile Administrator Configuration Guide

Version 9.7

October 2014

This document applies to webMethods Mobile Administrator Version 9.7 and to all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Document ID: MA-CG-97-20141015

Table of Contents

About This Guide

This guide explains how to configure webMethods Mobile Administrator and its mobile application build environment. The information in this guide is useful for system administrators, developers, and users who want to build mobile applications and manage mobile devices for Android, iOS and Windows Phone platforms.

Document Conventions

Convention	Description
Bold	Identifies elements on a screen.
Narrowfont	Identifies storage locations for services on webMethods Integration Server, using the convention *folder.subfolder:service* .
UPPERCASE	Identifies keyboard keys. Keys you must press simultaneously are joined with a plus sign (+).
Italic	Identifies variables for which you must supply values specific to your own situation or environment. Identifies new terms the first time they occur in the text.
`Monospace font`	Identifies text you must type or messages displayed by the system.
{ }	Indicates a set of choices from which you must choose one. Type only the information inside the curly braces. Do not type the { } symbols.
|	Separates two mutually exclusive choices in a syntax line. Type one of these choices. Do not type the | symbol.
[ ]	Indicates one or more options. Type only the information inside the square brackets. Do not type the [ ] symbols.
...	Indicates that you can type multiple options of the same type. Type only the information. Do not type the ellipsis (...).

Documentation Installation

You can download the product documentation using the Software AG Installer. The documentation is downloaded to a central directory named _documentation in the main installation directory (SoftwareAG by default).

Online Information

Software AG Documentation Website

You can find documentation on the Software AG Documentation website at http://documentation.softwareag.com. The site requires Empower credentials. If you do not have Empower credentials, you must use the TECHcommunity website.

Software AG Empower Product Support Website

You can find product information on the Software AG Empower Product Support website at https://empower.softwareag.com.

To submit feature/enhancement requests, get information about product availability, and download products and certified samples, go to Products.

To get information about fixes and to read early warnings, technical papers, and knowledge base articles, go to the Knowledge Center.

Software AG TECHcommunity

You can find documentation and other technical information on the Software AG TECHcommunity website at http://techcommunity.softwareag.com. You can:

- Access product documentation, if you have TECHcommunity credentials. If you do not, you will need to register and specify "Documentation" as an area of interest.
- Access articles, demos, and tutorials.
- Use the online discussion forums, moderated by Software AG professionals, to ask questions, discuss best practices, and learn how other customers are using Software AG technology.
- Link to external websites that discuss open standards and web technology.

1 Managing Licenses, Users and Groups

Overview

This chapter explains how to add licenses and manage users and groups in webMethods Mobile Administrator. You must complete different configuration steps for each mobile platform. To filter the steps required to configure a feature for a specific platform, use the platform selection menu on the **Configuration Assistant** page.

Note: You can return to the domain configuration page at any time during the configuration process by clicking the green notice field located at the top of each Mobile Administrator page. When a configuration step is completed, Mobile Administrator displays a check mark next to the configuration step.

About Adding Mobile Administrator Licenses

You must provide a valid license for Mobile Administrator. The expiration date and the number of users, applications and devices supported by Mobile Administrator depend on the license you use. If you need to extend the capacities or the expiration date of your first active license, you can extend that license by adding additional licenses.

Note: You cannot add the same license twice.

Software AG recommends that you add a new license before the currently valid license expires. Mobile Administrator automatically switches to the new license when the old license expires. When the new license is active, you can remove the old one.

Adding a License

To add a license

1. In Mobile Administrator, click  and select **Domain**. The **Domain Details** page opens.
2. In the **webMethods Mobile Administrator Licenses** section, click **Active Licenses**. The **All Licenses** page opens.
3. Click **Add License**.
4. Paste the license and then click **Add License**.

About Managing Mobile Administrator Users and Groups

You can create local users, or you can define Mobile Administrator users from an LDAP system. The default user has the following credentials in Mobile Administrator:

- User Name: admin

- Password: admin

When you create a user, either as a local user or from LDAP, you can grant site-level permissions to that user. To grant application-level permissions to a user, you must go to the application and modify permissions there. You can create and edit groups, and add users to them.

Important: Only users with **Manage Users and Groups** permissions can manage other user accounts, groups and site-level permissions.

About LDAP Users

You create LDAP users by connecting to an existing LDAP system. After you create the connection to the LDAP system, you log on Mobile Administrator with the LDAP user account. When an LDAP user logs on Mobile Administrator for the first time, all groups that the user is a member of are added to Mobile Administrator. After the user logs on Mobile Administrator for the first time, you can set the site-level permissions for the user. You cannot modify an LDAP user name or password in the Mobile Administrator instance. You update user credentials in the LDAP directory. Every time the LDAP user logs on, the LDAP group membership updates.

Adding Users

You can add users to Mobile Administrator by defining a local user or by adding users already defined in an LDAP system.

Adding a Local User

Only users with **Manage Users and Groups** permissions can add local users.

To add a local user

1. In Mobile Administrator, click ⚙ and select 👤. The **All Users** page opens.
2. Click +. The **New User** page opens.
3. Specify values for all fields and click **Create User.**

   Note: The **Active** check box is selected by default. Do not disable it.

Adding a User from an LDAP System

Only users with **Manage Users and Groups** permissions can add LDAP users.

To add a user from an LDAP system

1. In Mobile Administrator, click ⚙ and select **Domain**. The **Domain Details** page opens.
2. Click **Edit Domain**. The **Update Domain** page opens.

3. Scroll down to the **LDAP Configuration** section and specify the LDAP user details.
4. Click **Update Site**.

After you create a connection to the LDAP system, users can log on Mobile Administrator with the user name and password credentials stored for them in the LDAP system.

Editing User Details

Only users with **Manage Users and Groups** permissions can edit user details and site-level permissions.

To edit a user

1. In Mobile Administrator, click ⚙ and select **Users**. The **All Users** page opens.
2. Select the user that you want to update and click **Edit User**.
3. Specify values for the fields you want to update and click **Update User**.

Deleting Users

Only users with **Manage Users and Groups** permissions can delete users.

To delete a user

1. In Mobile Administrator, click ⚙ and select **Users**. The **All Users** page opens.
2. Select the user you want to delete and click **Delete**.

Creating Groups

Only users with **Manage Users and Groups** permissions can create groups.

To create a group

1. In Mobile Administrator, click ⚙ and select **Groups**.
2. Click +.
3. Specify the name of the group and click **Create User Group**.

Adding Users to Groups

Only users with **Manage Users and Groups** permissions can add users to groups.

To add a user to a group

1. In Mobile Administrator, click ⚙ and select **Users**.

2. Select the user you want to add.
3. Click **Add to Group** and select the group in which you want to add the user.

Removing Users from Groups

Only users with **Manage Users and Groups** permissions can remove users from groups.

To remove a user from a group

1. In Mobile Administrator, click and select **Users**.
2. Select the user you want to remove.
3. Click **Remove from Group** and select the group from which you want to remove the user.

Editing Groups

Only users with **Manage Users and Groups** permissions can edit groups.

To edit a group

1. In Mobile Administrator, click and select **Groups**.
2. Select the group you want to edit and click **Edit User Groups**.
3. Specify the name of the group in the **Name** field and click **Update User Group**.

Deleting Groups

Only users with **Manage Users and Groups** permissions can delete groups.

To delete a group

1. In Mobile Administrator, click and select **Groups**.
2. Select the group you want to delete and click **Delete**.

2 Configuring the Build Environment

About Configuring the Build Environment

To prepare webMethods Mobile Administrator to build mobile applications, you must configure the build environment with the necessary application signing certificates and profiles. After setting up the certificate signing, you connect one or more Mobile Administrator build nodes to execute the mobile build process.

Working with Certificates and Profiles

You must provide the appropriate certificates, profiles, and tokens for the supported platforms.

Configuring Certificate Signing on Android

When building applications for Android, you must provide a signing certificate.

Uploading Android Certificates

To upload an Android developer certificate

1. In Mobile Administrator, click and select **Developer Certificates**. The **All Certificates** page opens.
2. Click .
3. Select the Android platform and upload the P12 file.

Configuring Certificate Signing on iOS

To sign an application on iOS, first you must upload an iOS developer certificate that matches a provisioning profile. If Mobile Administrator cannot find a matching certificate, the upload of the provisioning profile fails. For more information about uploading an iOS developer certificate, see "Uploading an iOS developer certificate" on page 15.

Creating an iOS developer certificate

To create an iOS developer certificate

1. In Mobile Administrator, click and select **Developer Certificates**. The **All Certificates** page opens.
2. Click and select **New iOS Distribution Certificate**.
3. Click the certificate signing request to download it.
4. Sign the certificate signing request in the iOS provisioning portal.

5. In Mobile Administrator, click **Browse** to locate the iOS Distribution Certificate and then select **Upload Certificate**.

Uploading an iOS developer certificate

To upload an iOS developer certificate

1. In Mobile Administrator, click ⚙ and select **Developer Certificates**. The **All Certificates** page opens.
2. Click +.
3. Select the iOS platform and upload the P12 file.

Uploading an iOS Provisioning Profile

To add a provisioning profile to Mobile Administrator

1. In Mobile Administrator, click ⚙ and select **Provisioning Profiles**. The **All iOS Provisioning Profiles** page opens.
2. Click +.
3. Upload the .mobileprovision file.

Configuring Certificate Signing on Windows Phone

When registering for the Windows Phone Dev Center, you receive a Windows Phone 8 Application Enrollment Token file to configure Windows Phone 8 devices for the installation of enterprise applications. You must upload a file in the P12 format that contains a matching certificate and a private key.

Uploading the Windows Phone 8 Application Enrollment Token

To upload a Windows Phone 8 application enrollment token

1. In Mobile Administrator, click ⚙ and select **Domain**. The **Domain Details** page opens.
2. Click **Edit Domain**. The **Update Domain** page opens.
3. In the **Windows Phone 8 application enrollment token** field upload the AETX file. Click **Update Site**.

Uploading Windows Phone Certificates

To upload a Windows Phone developer certificate

1. In Mobile Administrator, click ⚙ and select **Developer Certificates**. The **All Certificates** page opens.
2. Click +.
3. Select **Windows Phone** and upload the P12 file.

Deleting Certificates

To delete certificates

1. In Mobile Administrator, click and select **Developer Certificates**. The **All Certificates** page opens.
2. Select the certificate you want to delete and click **Delete**.

Note: Only users with **Manage Site** permissions can delete certificates.

Connecting a Build Node to a Backend

The Mobile Administrator Build Node for Mac OS X supports building mobile applications for iOS and Android. The Windows 8 Build Node supports building applications for Windows Phone and Windows RT.

Connecting a Mac OS X Build Node

To set up a build node on Mac OS X

1. In Mobile Administrator, click and select **Build Nodes**. The **All Build Nodes** page opens.
2. Download the Mac OS X build node file and extract the downloaded file.
3. Launch the extracted application.
4. In the AppFresh Build Node wizard, go to the **Install** tab and perform the available steps.
5. On the **Build Node** tab, click to connect the build node to a backend.
6. Specify the Mobile Administrator host name without https://, and your user name and password.
7. Make sure the newly added host name and authentication token show up in the **Servers** list.
8. Click **Start**.

Note: To obtain debug information about the build node, click **Show Log File** and check the log.

Connecting a Windows 8 Build Node

To setup a build node on Windows 8 Pro

1. In Mobile Administrator, click and select **Build Nodes**. The **Build Nodes** page opens.
2. Click the Windows 8 build node link and download the file.

3. Run the downloaded installer file and follow the installation process.
4. Launch the build node application.
5. In the AppFresh Windows wizard, click **Add** to connect the build node to a backend.
6. Specify the Mobile Administrator host name without https://, and your user name and password.
7. Make sure the newly added server name and authentication token show up in the **Servers** list.
8. Click **Start**.

3 Building Mobile Applications

Overview

This chapter describes how to create build configurations, build App Store clients, and install the clients on mobile devices. After you configure the build environment, you can build mobile applications using webMethods Mobile Administrator. Before building mobile applications, you can build an App Store client for each mobile platform. You use the App Store client to browse and download applications. The App Store client is optional.

Important: Building and using an App Store client is required only when you want to use mobile device management (MDM) on iOS or Android. After you create an App Store client, you must install it on your mobile devices.

The following table shows the tasks you should perform to build the App Store client.

Task	For more information, see...
Creating a build configuration	"Creating Build Configurations" on page 20
Building an App Store client	"Building an App Store Client" on page 22
Installing an App Store client	"Installing the App Store on a Mobile Device" on page 22

Creating Build Configurations

Creating Build Configurations on Android

Before you can create an Android build configuration for a client application, make sure that you have uploaded a valid Android certificate. For more information about Android certificates, see "Uploading Android Certificates" on page 14.

To create an Android build configuration for a client application

1. In Mobile Administrator, click and select **App Store Client**.
2. On the **Build** tab, click . The **New Build Configuration** page opens.
3. Select the Android platform and one of the uploaded Android certificates.
4. Click **Create Build Configuration**.

Creating Build Configurations on iOS

Before you create an iOS build configuration for a client application, make sure that you have uploaded a valid iOS developer certificate and provisioning profile. Verify that the Bundle ID associated with one of the uploaded iOS provisioning profiles matches the iOS Bundle ID configured for the client application. For more information about iOS developer certificates, see "Uploading an iOS developer certificate" on page 15.

Verifying the Bundle ID

To verify the iOS Bundle ID of the client application

1. In Mobile Administrator, click and select **App Store Client**.
2. Click **Edit**. The **Edit App** page opens.
3. Under **iOS Bundle ID**, verify and update the bundle ID to a value that matches a provisioning profile, if necessary.
4. Click **Update App**.

Creating the iOS Build Configuration

To create an iOS build configuration for the client application

1. In Mobile Administrator, click and select **App Store Client**.
2. Click the **Build** tab and select . The **New Build Configuration** page opens.
3. Select the iOS platform and make sure one of the uploaded iOS provisioning profiles is displayed under **iOS Provisioning Profile.**

   Note: If none of the uploaded iOS provisioning profiles are displayed under **iOS Provisioning Profile**, none of them match the iOS Bundle ID of the client application.

4. Click **Create Build Configuration**.

Creating Build Configurations on Windows Phone

Before you can create a Windows Phone build configuration for a client application, make sure you have uploaded a valid Windows Phone certificate. For more information about Windows Phone certificates, see "Uploading Windows Phone Certificates" on page 15.

To create a Windows Phone build configuration for the client application

1. In Mobile Administrator, click and select **App Store Client**.
2. Go to the **Build** tab and click .

3. On the **New Build Configuration** tab select the Windows Phone platform and one of the uploaded Windows Phone Certificates under **Code Signing Certificate**.
4. Click **Create Build Configuration**.

Building an App Store Client

To launch a build job

1. In Mobile Administrator, click and select **App Store Client**.
2. Click the **Build** tab.
3. Select the build configurations for all the platforms for which you want to build a client and click **Launch Selected Build Configurations**.

Mobile Administrator generates a build job for each build configuration and platform. The build jobs remain in **Running** status for a while as the backend creates the source code for the client applications. When in **Success** status, the build jobs are ready to be processed by any online build nodes. You can go to the **Versions** tab to view build configuration information, such as platform, version, and date.

Installing the App Store on a Mobile Device

You can log on Mobile Administrator on a mobile device to browse the App Store. However, Software AG recommends downloading the native App Store client. On each supported device, the Mobile Administrator logon page shows a direct download link for the native App Store client.

To install the app store client on a mobile device

1. Go to the Mobile Administrator URL on the mobile device.
2. Click the download link on the logon page.
3. Follow the instructions of the mobile operating system to install the application.

4 Configuring Mobile Device Management

Overview

Before you can use mobile device management (MDM) with webMethods Mobile Administrator, you must create an iOS MDM Certificate.

Creating an iOS MDM Certificate

To support MDM on iOS devices, you must create a certificate in the Mobile Administrator backend signed by Apple.

To create an iOS MDM certificate

1. In Mobile Administrator, click  and select **Domain**. The **Domain Details** page opens.
2. Select the domain for which you want to provide the license.
3. In the **MDM Certificates** section, click **New Certificate**. The **Certificate** page opens.
4. Click the certificate signing request to download it.
5. Sign the certificate signing request.
6. Click **Browse** to locate the MDM certificate and click **Upload Certificate**.

Adding a GCM API Key

To support MDM and push notifications on Android devices, you must configure an API key for the Google GCM API in the Mobile Administrator backend. For details about how to create the API key, see the Google Android documentation.

To configure the API key in Mobile Administrator

1. In Mobile Administrator, click  and select **Domain**. The **Domain Details** page opens.
2. Click **Edit Domain**. The **Update Domain** page opens.
3. In the **GCM API Key** field, specify the API key.
4. Click **Update Site**.