



# Infor LN Mobile Service for Android and iOS

Getting Started (version 2.6)

### **Important Notices**

The material contained in this publication (including any supplementary information) constitutes and contains confidential and proprietary information of Infor.

By gaining access to the attached, you acknowledge and agree that the material (including any modification, translation or adaptation of the material) and all copyright, trade secrets and all other right, title and interest therein, are the sole property of Infor and that you shall not gain right, title or interest in the material (including any modification, translation or adaptation of the material) by virtue of your review thereof other than the non-exclusive right to use the material solely in connection with and the furtherance of your license and use of software made available to your company from Infor pursuant to a separate agreement, the terms of which separate agreement shall govern your use of this material and all supplemental related materials ("Purpose").

In addition, by accessing the enclosed material, you acknowledge and agree that you are required to maintain such material in strict confidence and that your use of such material is limited to the Purpose described above. Although Infor has taken due care to ensure that the material included in this publication is accurate and complete, Infor cannot warrant that the information contained in this publication is complete, does not contain typographical or other errors, or will meet your specific requirements. As such, Infor does not assume and hereby disclaims all liability, consequential or otherwise, for any loss or damage to any person or entity which is caused by or relates to errors or omissions in this publication (including any supplementary information), whether such errors or omissions result from negligence, accident or any other cause.

Without limitation, U.S. export control laws and other applicable export and import laws govern your use of this material and you will neither export or re-export, directly or indirectly, this material nor any related materials or supplemental information in violation of such laws, or use such materials for any purpose prohibited by such laws.

### **Trademark Acknowledgements**

The word and design marks set forth herein are trademarks and/or registered trademarks of Infor and/or related affiliates and subsidiaries. All rights reserved. All other company, product, trade or service names referenced may be registered trademarks or trademarks of their respective owners.

### **Publication Information**

Release: Infor LN Mobile Service for Android and iOS

Publication date: November 22, 2021

---

---

# Contents

About this guide .....	5
Intended audience .....	5
Contacting Infor.....	5
<b>Chapter 1 Introduction and specifications.....</b>	<b>7</b>
Introduction .....	7
LN Specifications .....	7
Device Specifications.....	7
Android: .....	7
iOS: .....	8
<b>Chapter 2 Data Setup in LN .....</b>	<b>9</b>
Enabling the LN Client Service in LN-UI .....	9
Activating Mobile Service .....	10
Setting up Service Employee Data .....	10
Providing connection settings.....	11
Defining Mobiles Service App Settings in LN.....	12
<b>Chapter 3 Mobile Service Installation and Configuration .....</b>	<b>13</b>
Installation.....	13
Configuration .....	13
Entering environment settings manually.....	14
Loading a file with environment settings.....	15
Scanning environment settings with a QR code.....	15
Set environment settings by selecting a Managed Server .....	16
<b>Chapter 4 First Time Sign In .....</b>	<b>17</b>
<b>Chapter 5 Synchronization .....</b>	<b>19</b>
Latest changes log .....	19
Synchronization icon .....	20

	Synchronization errors .....	22
<b>Chapter 6</b>	<b>Important Settings .....</b>	<b>23</b>
<b>Chapter 7</b>	<b>Documents.....</b>	<b>24</b>
<b>Chapter 8</b>	<b>ION API .....</b>	<b>25</b>
	Create an Authorized App.....	25
	Get the credentials .....	26
<b>Chapter 9</b>	<b>Mobile Device Management .....</b>	<b>27</b>
	Managed Servers.....	27
	Allow Custom Server List.....	27
	Force Passcode .....	28
	MDM Keys and Values.....	28
	Android app restrictions file.....	29
	iOS app configuration file .....	31

---

## About this guide

This document describes the process to install and configure the Infor LN Mobile Service for Android app or the Infor LN Mobile Service for iOS app.

It also describes the minimum configuration of LN to be done by the system administrator before the Mobile Service app can be used.

## Intended audience

This guide is intended for:

- Users of Infor LN Mobile Service for Android app,
- Users of Infor LN Mobile Service for iOS app,
- LN system administrators.

## Contacting Infor

If you have questions about Infor products, go to the Infor Support Portal at [www.infor.com/inforxtreme](http://www.infor.com/inforxtreme).

If we update this document after the product release, we will post the new version on this web site. We recommend that you check this web site periodically for updated documentation.

The latest solutions with new functionality and bug fixes are always published on the Infor Support Portal under [KB 1645209](#)

If you have a question about the functionality of Infor LN Mobile Service, you may also contact us via mail: [ln.mobile.service@infor.com](mailto:ln.mobile.service@infor.com)

If you have comments about Infor documentation, contact [documentation@infor.com](mailto:documentation@infor.com).



## Introduction

Infor LN Mobile Service for Android/iOS provides extensive field service functionality on Android and iOS mobile devices. It is not a stand-alone application, but fully integrates with Infor LN, both on premise and in the cloud.

## LN Specifications

Infor LN Mobile Service for Android/iOS is supported on Infor LN 10.4, 10.5.2, 10.5, 10.6, 10.7 and LN Cloud Edition.

LN Mobile Service provides the most functionality when integrated with LN Cloud Edition. It provides less functionality when integrating with earlier versions of LN, the least functionality when integrating with LN 10.4.

A named user license for **license id 7135** is required to connect Mobile Service to LN.

**Solution 2030725** must have been installed when using LN version 10.4, 10.5, 10.5.2 or 10.6.

## Device Specifications

### Android:

Infor LN Mobile Service for Android is supported on any Android device with Android 7.1 or later, **except** for the following:

- Android TV
- Wear OS
- Any device that is not certified by Google.

It is designed to run on a mobile phone but will also run on tablets and Chromebooks.

Infor advises devices which at least adhere to the following specifications:

- Resolution: 720x1280 pixels, 16:9 ratio (320 dpi)
- Internal memory 16GB, 1.5 GB RAM
- Free storage capacity: 6GB, but this heavily depends on the amount of data in the LN database relevant to Infor LN Mobile Service.
- 8 MP camera.
- GPS: Yes

### **iOS:**

Infor LN Mobile Service for iOS is supported on any iPhone or iPad with iOS 8.0 or later. tvOS and watchOS are not supported.

- Supported processor architectures:
  - ARMv7
  - ARM64

It is designed to run on an iPhone but will also run on iPads.

Infor advises devices which at least adhere to the following specifications:

- Screen size: 5,5 inch (diagonal).
- Free storage capacity: 6GB, but this heavily depends on the amount of data in the LN database relevant to Infor LN Mobile Service.
- 8 MP camera.
- GPS: Yes



## Chapter 2 Data Setup in LN

# 2

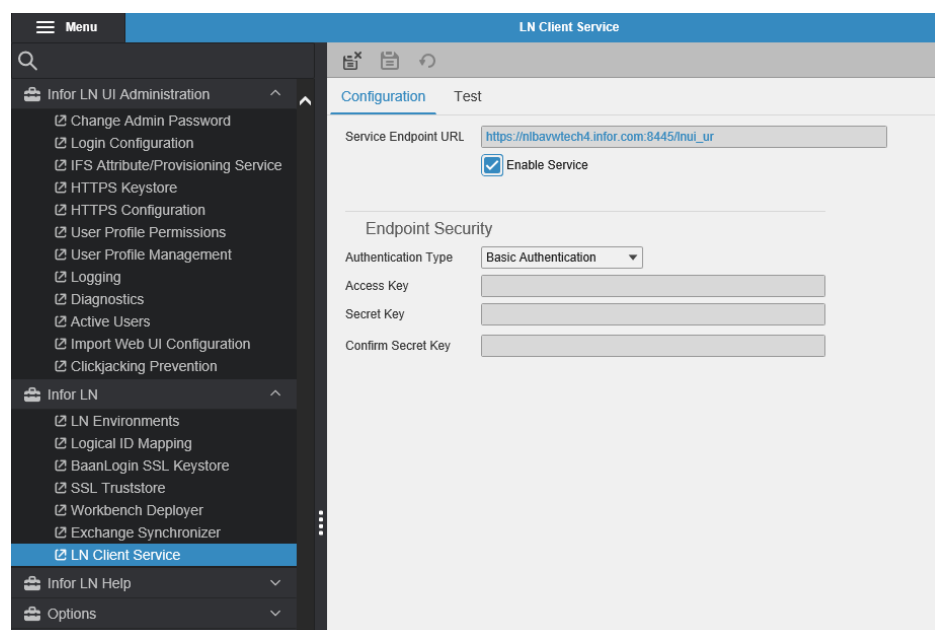
Some data must be set up before Infor LN Mobile Service can be used. The LN Client Service in LN-UI must be enabled, Mobile Service must be activated, and a minimum set of data per service employee must be set up.

### Enabling the LN Client Service in LN-UI

To enable the LN Client Service, complete the following steps:

1. Start the Admin Page of LN-UI.
2. Go to Infor LN.
3. Select LN Client Service.
4. Select the Enable Service check box.

You can use the Test tab to test the connection.



Note: for LN Cloud Edition this service is by default enabled.

## Activating Mobile Service

To activate Mobile Service, complete the following steps:

1. Start the Infor LN application and select the company to work in.
2. Start the *Implemented Software Components* (tccom0500m000) session.
3. Open the company for which Mobile Service must be activated.
4. Check the Mobile Field Service check box:

The screenshot shows the 'Implemented Software Components' window. The 'Description' field is set to 'Actual set'. The 'Company' field is set to '0551 infor'. The 'Archive Company' field is set to '0552 archive company for 551'. The 'Integrations' tab is selected, and the 'Mobile Field Service' checkbox is checked.

## Setting up Service Employee Data

To make it possible for a service employee to use Mobile Service, complete the following steps:

1. Start the Employee 360 session (bpmdm0101m100) and add at least the following details for the employee:
  - a **Logon Code:** Specify a LN user name.
  - b **Department:** Specify the Department. This department must exist in the Service Departments (tsmdm1100m000).
  - c **People Data:** Set the value to Yes.
  - d **Service Data:** Set the value to Yes.
2. Start Service User Profiles (tsmdm1150m000) to add a profile.
  - a Click Add
  - b Specify the Login Code
  - c Specify the LN user name.

- d Based on your settings, the value of the Service Engineer and Service Department fields are defaulted.
- e Click Save.

The service employee can now use Infor LN Mobile Service.

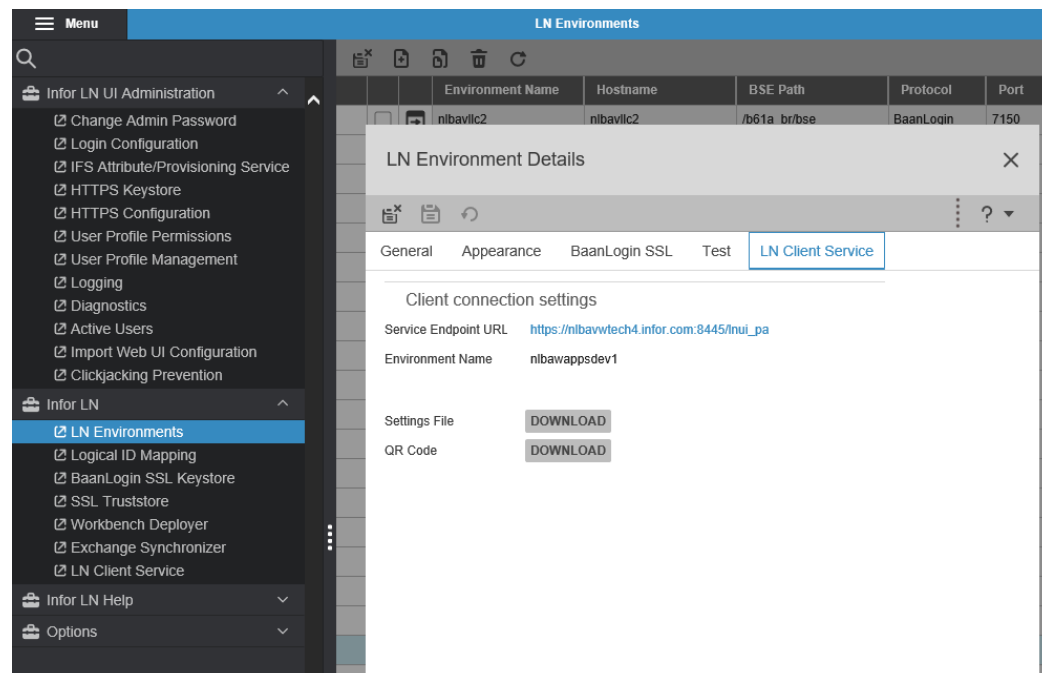
Note: besides the user profile, a Service User Template (tsmdm1160m000) can be defined which contains additional settings for Mobile Service. This template can be linked to the applicable User Profile(s).

## Providing connection settings

In the Mobile Service application, a user must first set up a profile and an environment, before the application can be used. The environment connection settings can be provided in the following ways:

- The user can enter the connection settings manually.
- The user can load a connection settings file to fill the connection settings.
- The user can scan a QR code to fill the connection settings.
- The user can select a Managed Server (only when Mobile Service is managed by a Mobile Device Management solution).

The settings file or QR code must be provided by the system administrator. These can be downloaded from the LN Environment Details in the LN-UI admin page:



Note: to set up a connection with authentication via ION API (for example when connecting to LN in a multi-tenant environment), you must either load a settings file or scan a QR code. These cannot be retrieved from the LN Environment Details but can be retrieved from the ION API Authorized Apps page. Refer to chapter ION API.

## Defining Mobiles Service App Settings in LN

There are various settings which can be set in the Mobile Service application itself. This allows service employees to change the behavior and look of the app and enable or disable certain functionality. In practice, the desired settings are often the same for all service employees of a certain company. In addition, a company might also want to prevent service employees from changing certain settings.

Within LN, these Mobile Service app settings can be defined in one or more setting files. A setting file can be linked to a service user template. These settings will be used as a default when a service employee starts using Mobile Service. Some settings might also be made read-only, preventing service employees from changing the setting in the Mobile Service application.

The use of app setting files is optional. Details of the setup are given in the Infor LN Mobile Service User Guide.

## Chapter 3 Mobile Service Installation and Configuration

# 3

### Installation

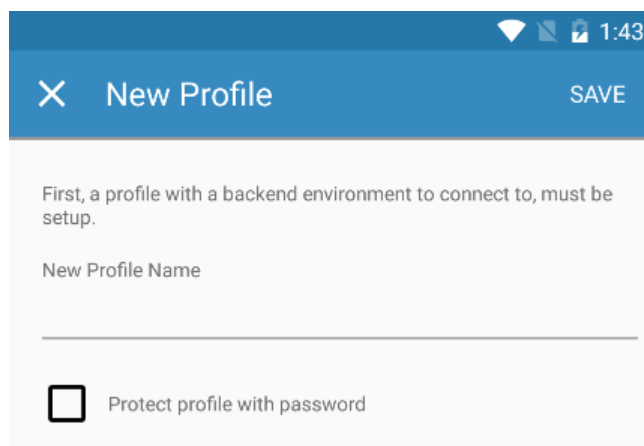
Execute the following steps to install Infor LN Mobile Service:

1. Start Google Play Store (Android) or App Store (iOS) on your device.
2. Search for 'Infor LN Mobile Service'.
3. If found, download and install it.
4. Accept the permissions, if asked for.
5. Open the app after installation has completed.

### Configuration

Before the app can be used it must be configured once with a new profile.

When the app starts, it displays the New Profile screen:

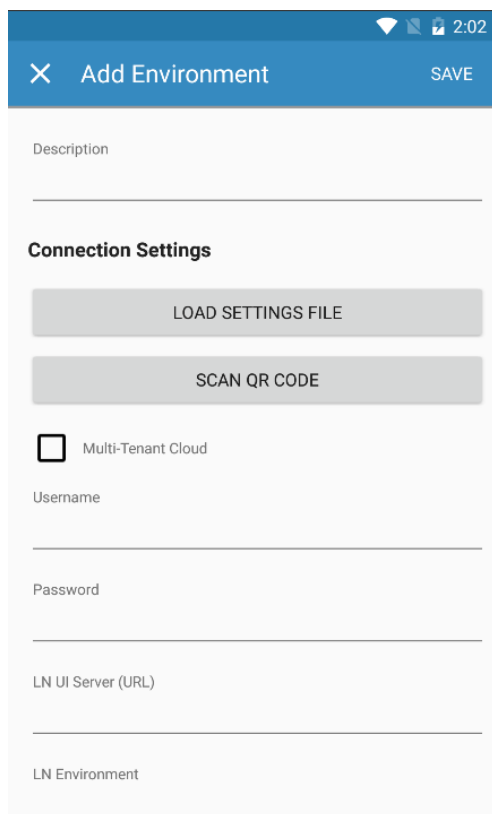


1. Enter a new profile name. This can be any name you want, for example your own name.
2. To protect the profile with a password, check the 'Protect profile with password' checkbox and enter a password.

Note: this password is the local profile password that is used to sign in into the application. It

does not have to be the same as the password to connect to the Infor LN backend. It is not mandatory to protect the profile with a password.

3. Press Save.
4. The Add Environment screen is displayed. An environment holds all application data and



settings related to one LN backend. In this screen an environment description and the settings that are needed to connect to the LN backend, need to be defined.

5. Enter a description. This can be anything you want, for example LN Service or Service Company 1234.
6. There are several options to provide the connection settings:
  - a Enter them manually.
  - b Load a settings file.
  - c Scan a QR code.
  - d Selecting a Managed Server

Note: to set up a connection with authentication via ION API, you must either load a settings file, scan a QR code or select a Managed Server.

### Entering environment settings manually

Your system administrator provided you with the settings.

Enter the following settings:

1. Your username and password.  
In most cases the username and password are your Single Sign On username and password.  
Note: You may have to prepend the domain with the username, for example infor\<your username>.
2. LN UI Server (URL)
3. LN Environment
4. Company
5. Select 'Save'. The Sign In screen displays.

### **Loading a file with environment settings**

Your system administrator provided you with a settings file. Make sure you have this file on your device or that you can retrieve it from a cloud location (for example Google Drive or iCloud).

Complete the following steps:

1. Press 'Load Settings File'.
2. Browse to the location where the settings file is stored and select it.
3. The settings are imported from the selected file.
4. Enter your username and password (except when authentication must be performed via ION API).  
In most cases the username and password are your Single Sign On username and password.  
Note: You may have to prepend the domain with the username, for example infor\<your username>.
5. Enter the company number if it is not already filled.
6. Press 'Save'. The Sign In screen displays.

### **Scanning environment settings with a QR code**

Your system administrator provided you with a QR code, for example as a picture in your mail or an URL to a site that displays the QR code. Make sure you have this displayed on a screen or in printed format.

Complete the following steps:

1. Press 'Scan QR code'.
2. Scan the QR code.
3. The settings are imported.

4. Enter your username and password (except when authentication must be performed via ION API).  
In most cases the username and password are your Single Sign On username and password.  
Note: You may have to prepend the domain with the username, for example infor\<your username>.
5. Enter the company number if it is not already filled.
6. Press 'Save'. The Sign In screen displays.

### **Set environment settings by selecting a Managed Server**

When your organization uses a Mobile Device Management (MDM) solution the connection settings can be supplied with or to Mobile Service. If this is the case the connection settings screen shows another field called Managed Server.

Complete the following steps:

1. Select a Managed Server.
2. Enter your username and password (except when authentication must be performed via ION API; these fields are not available then). In most cases the username and password are your Single Sign On username and password. Note: You may have to prepend the domain to the username, for example infor\<yourusername>.
3. Enter the company number if it is not already filled.
4. Press 'Save'. The Sign In screen displays.

For additional information on how to setup the connection settings via Managed Servers refer to Chapter 8.

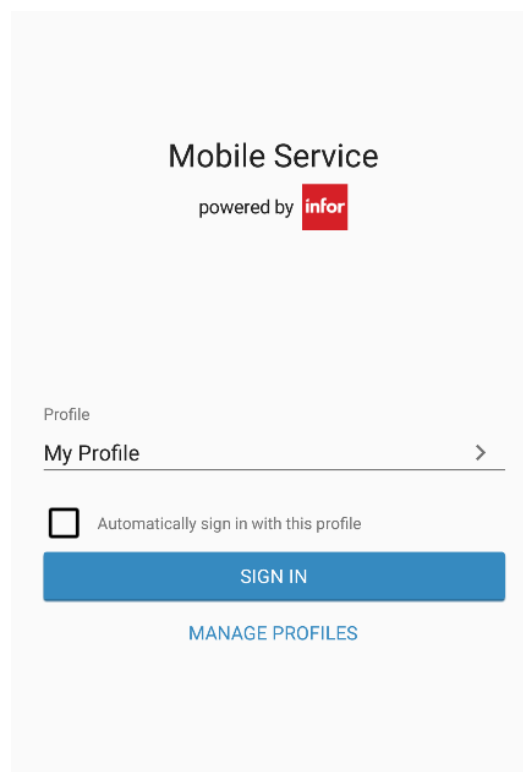


## Chapter 4 First Time Sign In

# 4

Perform the following steps the first time you sign in into the Mobile Service application:

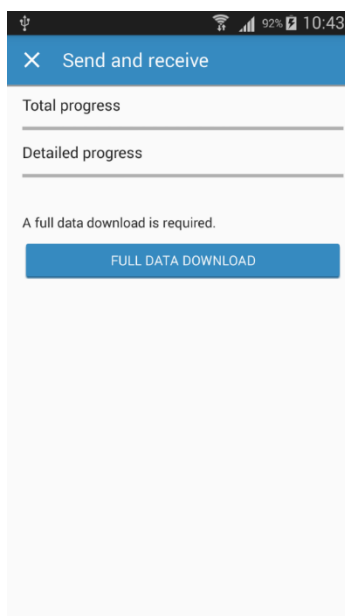
- Make sure your device is online.
- Start Infor LN Mobile Service on your device.
- The Sign In screen displays:



- Select your profile,
- Enter your profile password, if necessary.
- Optionally select 'Automatically sign in with this profile'.  
When this option is selected, the app will not ask for your profile or profile password anymore and automatically sign in the next time you start the app.
- Press Sign In.  
The app will sign in and will connect to LN. This may take a while when starting the app for the first time.  
Note: when authentication must be performed via ION API, a browser pops up, asking you to

provide your credentials (email and password) to the authentication server. Provide your credentials, press OK (or Sign In). A Request for Approval screen appears. Mobile Service will connect to LN after pressing the Allow button.

- The 'Send and Receive' screen will display.  
A full data download needs to be performed the first time you start the app. This action reads all required master data and your assigned activities from LN, and stores the data locally.



- Press 'Full Data Download'.
- Answer 'Yes' to the question 'Run a full data download?'.
- Wait until the download has completed (Total progress is 100%).  
Note: You may interrupt the full download if needed and resume it at a later moment.
- Close the Send and Receive screen.
- The Schedule screen is displayed and shows your assigned visits.
- Infor LN Mobile Service is now ready to use.

Note: a full data download is only required in the following situations:

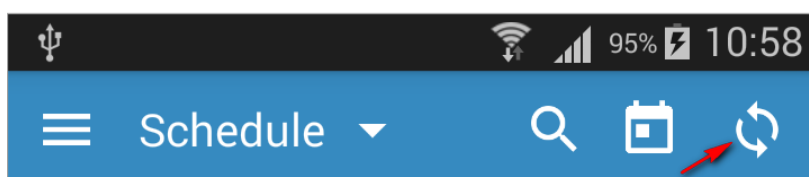
- **After installing Mobile Service for the first time.**  
All changes in Mobile Service that are done after the full data download are synchronized with LN during regular synchronizations. Also, all LN changes that are of interest to Mobile Service are synchronized with Mobile Service during these regular synchronizations. These regular synchronizations can be done manually or automatically.
- **If Mobile Service indicates this by means of a message.**  
This may for example occur when the retention period expires (see next chapter), or after an update of the Mobile Service application.

## Chapter 5 Synchronization

# 5

Data must be synchronized if it has changed in Infor LN Mobile Service or when relevant data in the LN backend has changed. This can be done manually or automatically.

A manual synchronization can be initiated at any moment by selecting the synchronization icon that is in the top right corner of the application:



Another way to initiate a manual synchronization is by pressing the menu icon, selecting Send/Receive, and then pressing the Send/Receive button.

To enable automatic synchronization, select the menu in the top left corner of the application, then select Settings, select Send/Receive and switch on 'Automatically'. Also, enter a receive interval. The receive interval determines how often the application will update the application with relevant changed data from LN, even if no data has been changed in Infor LN Mobile Service.

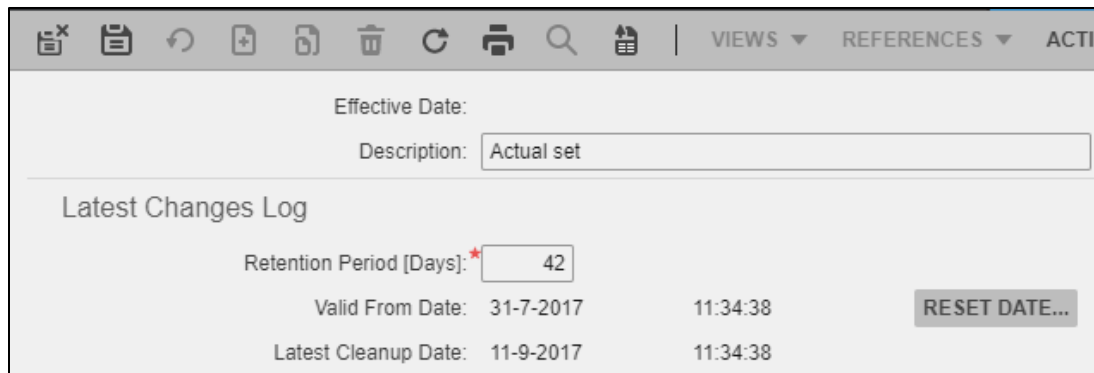
The application will synchronize data with LN at appropriate times if automatic synchronization is enabled. For example, if the application runs for a while without user interaction. This synchronization will only be done if data has been changed by the user in the application.

### Latest changes log

Changes in LN that need to be synchronized with Infor LN Mobile Service are based on the Latest Changes Log (tcgen3500m000). This log contains all objects that have changed and is used by Infor LN Mobile Service to download new information.

The log contains all objects that have changed during the so called 'Latest Changes Log Retention Period'. This Retention Period can be set in the Generic Parameters (tcgen0100m000).

Note: A new full data download is required when the number of days the last synchronization took place exceeds the retention period. The "Valid From Date" shows the date from which the Latest Changes Log is valid, mostly the current date minus the retention period.



Effective Date:

Description:

Latest Changes Log

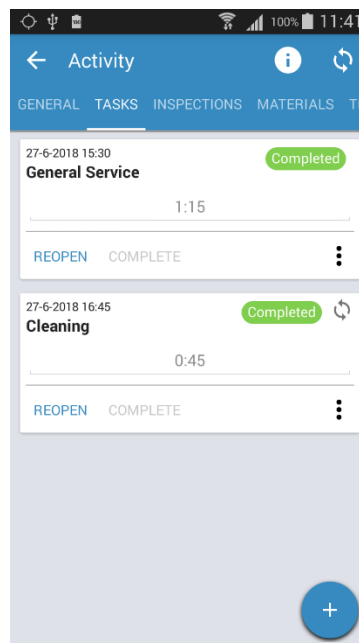
Retention Period [Days]:

Valid From Date: 31-7-2017 11:34:38 [RESET DATE...](#)

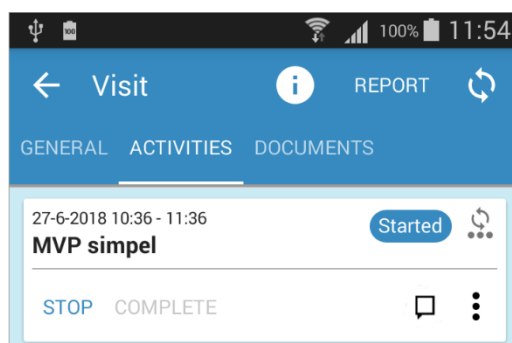
Latest Cleanup Date: 11-9-2017 11:34:38

## Synchronization icon

When changes are made in Infor LN Mobile Service, a synchronization icon will appear to indicate that data that has changed and must be synchronized. For example, the next picture shows two tasks. The data of the second task has changed:



The parent data of the data that has changed will show a different synchronization icon, indicating that one of its children has changed. See for example the next picture of the activity of the changed task:



Some changes must be submitted before they are synchronized with LN. This must be done in the following ways:

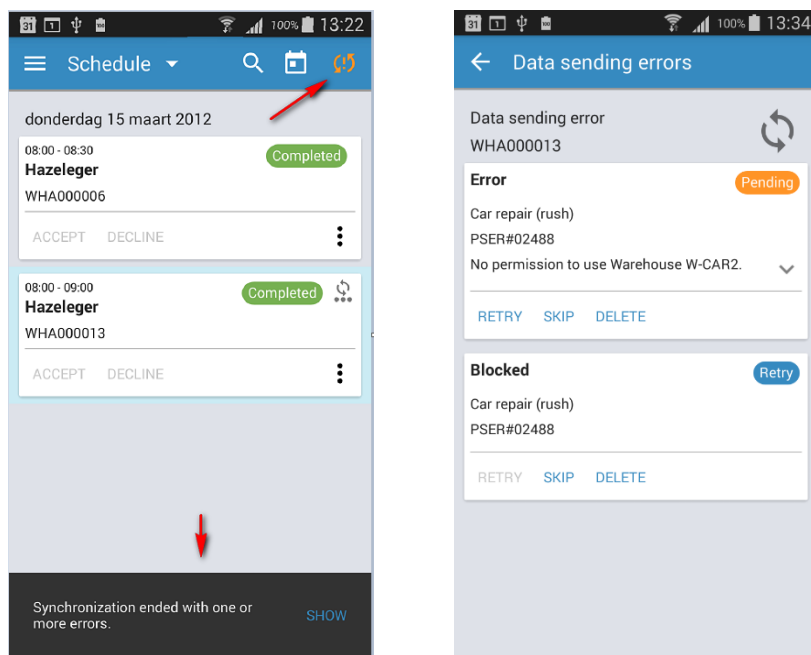
- Tasks and Inspections must be set to status Completed.
- Travel Time and Other Costs must be set to status Confirmed.
- Materials must be used, scrapped, returned or ordered.

The synchronization indicator will only disappear if the changes have been properly sent to LN.

The latest version of a service order cannot be shown in Mobile Service if not *all* changes of this service order have been properly sent to LN. In fact, any local change will block the download of the latest version of the service order from LN.

## Synchronization errors

Synchronization can sometimes result in errors. When this is the case, the synchronization icon will contain an exclamation mark and an alert will pop up:



When selecting the synchronization icon or 'Show' in the alert, the Data Sending Errors screen will display. It shows the changed objects that resulted into an error, including the error, and the remaining synchronizations that are blocked due to the error.

Choose one of the following actions to process the error:

- **Retry**  
This will try to synchronize the data again. This option may, for example, be used when data in LN has been corrected, and the correction makes it possible to synchronize the data again.
- **Skip**  
This will skip the synchronization of the data for now.
- **Delete**  
This will undo the changes that caused the error.

Select the synchronization icon after you selected the action to synchronize the (remaining) data again.

## Chapter 6 Important Settings

# 6

Infor LN Mobile Service contains settings to manage the behavior of the application. Click the option 'Settings' in the menu, to start the Settings screen.

It is recommended that you specify these settings, the first time you use the application:

- **Send/Receive - Automatically:**  
If switched on (blue), the application sends data that has been changed in the app at appropriate moments to LN. For example, when you do not use the app for a while. On the other hand, you can set the receive interval to define how often you want to receive changed data from LN.
- **Send/Receive - When activity paused or completed:**  
If switched on (blue), the application sends and receives data each time you pause or complete an activity.
- **Send/Receive - Send GPS Information:**  
If switched on (blue), the application sends GPS information at appropriate moments to LN, for example when starting or stopping an activity.
- **Data Display – Display format code and description fields:**  
For fields that have a code as well as a description (for example item), you can define how to display them. For example, only the code. Or only the description. Or both.  
You can enter one or more separator characters if you choose to display both. If you enter only a starting bracket or parenthesis alike character, then either the code or description is surrounded with these characters, depending on whether the code or the description is displayed last.  
Starting brackets that can be used are [, { and (.

## Chapter 7 Documents

# 7

Infor LN Mobile Service can download and upload documents to either 'Infor Document Management' or to the module 'Document Management' within Infor LN. Infor LN Mobile Service does not connect directly to these document management systems but connects to the Infor LN Document Hub.

To enable document uploads and downloads in Mobile Service, complete the following steps:

- 1 Initialize the Document Hub with session 'Initialize Document Hub' (ttdms3200m000). The application 'infor.ln.mfs' is created automatically and will become visible in session 'Applications' (ttdms3500m000)
- 2 Go to 'Document Mapping' (ttdms3550m100) and search for application 'infor.ln.mfs'.
- 3 Add at least one 'Document Type' for each 'Table Name' for which documents are applicable for Infor LN Mobile Service.

Make sure the 'Upload' and/or 'Download' fields and the 'Attribute Mapping' are setup properly.

- 4 Start Infor LN Mobile Service. The 'Document' interface is available if at least one of the 'Table Names' has a 'Document Type' for which 'Upload' and/or 'Download' is set to 'Yes'.



## Chapter 8 ION API

# 8

If authentication must be performed via ION API some actions are needed to enable the connection from Mobile Service to Infor LN. This is for example the case when Infor LN runs in a multi-tenant cloud environment.

### Create an Authorized App

The first action for the system administrator is to create an authorized app in ION API.

Note: in the latest versions of ION API this authorized app is already available with name LN Mobile Service. In this case it is not needed to create an authorized app anymore.

The following steps are needed to create an authorized app:

- 1 Start ION API.
- 2 Select Authorized Apps from the menu.
- 3 Click on the + button.
- 4 Enter a name, for example Mobile Service. Note that this name will be used as name for the credentials file that can be downloaded later.
- 5 Select Type “Mobile - Android” or “Mobile - iOS”.
- 6 Enter a description in the Description box, for example Mobile Service Application.
- 7 Enter a redirect URL, for example <http://localhost/mobileservice> or `com.infor.LN.MobileService://localhost/redirect`  
The url must be of the following format: `<some url scheme>://localhost/<url path>`
- 8 Enter the download URL:
  - Android: <https://play.google.com/store/apps/details?id=com.infor.Inmobileservice>
  - iOS: <https://itunes.apple.com/us/app/id1460805871>
- 9 Enter the package name (Android) or Bundle ID (iOS): `com.infor.Inmobileservice`
- 10 Enter the App Store ID (iOS only): `id1460805871`
- 11 Enter a refresh time for the OAuth 2.0 Access Token.
- 12 Keep option “Issue Refresh Tokens” enabled.
- 13 Enter a value for the “Refresh Token Grant Lifetime”, for example 8 hours. Enter 0 hours if the refresh token should never expire.

14 Click the Save button.

15 The Client ID and Secret are generated, and the authorized app is stored.

### **Get the credentials**

The next action is to download credentials file by clicking the button “Download Credentials”. A file named <name>.ionapi will be downloaded. This file must be uploaded in the “Environment Connection Settings” of the Mobile Service app to enable a connection with authentication via ION API.

Instead of downloading the credentials file it is also possible to send the QR code to the Mobile Service user. To populate the connection settings, the QR code can be scanned in in the “Add Environment” screen or the Environment Connection Settings screen of Mobile Service by clicking the “Scan QR Code” button.

## Chapter 9 Mobile Device Management

# 9

Mobile Service for Android and iOS can be managed by dedicated mobile device management (MDM) software. This allows an administrator to use MDM to set certain settings in mobile service.

Many settings of Mobile Service are controlled from LN. The settings in the Mobile Service application itself can also be controlled from LN through an app settings file. All these settings require Mobile Service to be connected to LN. There are however some settings which an administrator might want to set that must be implemented before any connection is made with LN. These settings can be set through mobile device management for Android and iOS.

The remainder of the chapter will give an overview of which MDM settings are supported by the Mobile Service application. It will also supply the exact keys and values which need to be set in the MDM provider to make use of this functionality.

There are many different MDM providers. Refer to the documentation of the provider on how to set these settings within the MDM software application.

The following settings are supported:

### Managed Servers

Managed Servers can be defined for users to connect to. A Managed Server contains a JSON object/strings with the server connection settings. The server can be a cloud server or an on-premise server. Using this functionality prevents the administrator from having to distribute QR-codes or connection settings files to users. Multiple managed servers can be defined allowing the users to connect to multiple environments.

**Note:** the connection settings can be retrieved from the LN Environment Details in the LN-UI admin page, or in case of authentication via IONAPI, from the Mobile Service Authorized App on the IONAPI Authorized Apps page (refer to chapter ION API).

### Allow Custom Server List

This is a setting that determines if any environments can be created in Mobile Service that are not part of the defined managed servers.

When set to false, the Mobile Service user can only create environments in the connection settings view of Mobile Service that connect to one of the defined managed servers. Scanning QR-Codes, reading setting files and manually entering or changing the relevant fields will not be possible. This will prevent users from connecting to any environment not set in the mobile device management system.

When set to true, the Mobile Service user can define its own connection settings, besides the defined managed servers.

---

Warning: When setting to false, all environments not matching a managed server will be deleted from Mobile Service. Take special care when using this setting when users are already using mobile service in the field.

## Force Passcode

Based on this setting Mobile Service profiles can be required to be protected by a password.

When set to true, the Mobile Service user must define a profile password when creating a new profile. When the user attempts to login to an existing profile that is not password protected, the user must first define a profile password before continuing.

When set to false, the user is not required to define a profile password.

## MDM Keys and Values

To make use of the settings that Mobile Service supports through MDM, the exact keys and values of these settings need to be entered in the MDM application.

The Force Passcode and Allow Custom Server List settings can only be set once, and the values of these settings are Boolean values.

For the Managed Server setting multiple servers can be entered. This can be done by using a key of the format "Managed Server X" where the X can be replaced by an integer. The value of each managed server setting must always be the a json string containing the connection settings to the LN environment.

The following table shows the supported keys:

Key	Datatype	Remark
"Force Passcode"	Boolean	
"Allow Custom Server List"	Boolean	
"Managed Server X"	String	<b>R1</b>

**R1:** X is replaced by an integer (for example "Managed Server 1", "Managed Server 4") to form the key, the value should contain a json string.

iOS: X can range from 1 to infinity, but for numbers higher than 9 there should be no gaps (example: to use 12 the numbers 10 and 11 should also be in use).

Android: X can range from 1 to 9.

---

## Android app restrictions file

Below is the xml definition of the android app restrictions. This xml file is also embedded within the mobile service app and can usually be read automatically from mobile service by the MDM software, which will aid in setting the correct MDM settings.

```
<?xml version="1.0" encoding="utf-8"?>
<restrictions xmlns:android="http://schemas.android.com/apk/res/android">
  <restriction
    android:key="Allow Custom Server List"
    android:restrictionType="bool"
    android:defaultValue="true"
    android:title="Allow Custom Server List"/>
  <restriction
    android:key="Force Passcode"
    android:restrictionType="bool"
    android:defaultValue="false"
    android:title="Force Passcode"/>
  <restriction
    android:key="Managed Server 1"
    android:restrictionType="string"
    android:defaultValue=""
    android:title="Managed Server 1"/>
  <restriction
    android:key="Managed Server 2"
    android:restrictionType="string"
    android:defaultValue=""
    android:title="Managed Server 2"/>
  <restriction
    android:key="Managed Server 3"
    android:restrictionType="string"
    android:defaultValue=""
    android:title="Managed Server 3"/>
  <restriction
    android:key="Managed Server 4"
    android:restrictionType="string"
    android:defaultValue=""
    android:title="Managed Server 4"/>
  <restriction
    android:key="Managed Server 5"
    android:restrictionType="string"
    android:defaultValue=""
    android:title="Managed Server 5"/>
  <restriction
    android:key="Managed Server 6"
    android:restrictionType="string"
    android:defaultValue=""
    android:title="Managed Server 6"/>
  <restriction
    android:key="Managed Server 7"
```

---

```
android:restrictionType="string"
android:defaultValue=""
android:title="Managed Server 7"/>
  <restriction
android:key="Managed Server 8"
android:restrictionType="string"
android:defaultValue=""
android:title="Managed Server 8"/>
  <restriction
android:key="Managed Server 9"
android:restrictionType="string"
android:defaultValue=""
android:title="Managed Server 9"/>
</restrictions>
```

---

## iOS app configuration file

Below is the xml definition of the iOS configuration file. The below content can be stored in an xml file. This xml file can then be imported into MDM software, which will aid in setting the correct MDM settings.

```
<?xml version="1.0" encoding="utf-8"?>
<managedAppConfiguration>
  <version>1</version>
  <bundleId>com.infor.Inmobileservice</bundleId>
  <dict>
    <boolean keyName="Allow Custom Server List">
      <defaultValue>
        <value>true</value>
      </defaultValue>
      <constraint nullable="true" />
    </boolean>
    <boolean keyName="Force Passcode">
      <defaultValue>
        <value>false</value>
      </defaultValue>
      <constraint nullable="true" />
    </boolean>
    <string keyName="Managed Server 1">
      <defaultValue>
        <value></value>
      </defaultValue>
      <constraint nullable="true" />
    </string>
    <string keyName="Managed Server 2">
      <defaultValue>
        <value></value>
      </defaultValue>
      <constraint nullable="true" />
    </string>
    <string keyName="Managed Server 3">
      <defaultValue>
        <value></value>
      </defaultValue>
      <constraint nullable="true" />
    </string>
    <string keyName="Managed Server 4">
      <defaultValue>
        <value></value>
      </defaultValue>
      <constraint nullable="true" />
    </string>
    <string keyName="Managed Server 5">
      <defaultValue>
        <value></value>
      </defaultValue>
    </string>
  </dict>
</managedAppConfiguration>
```

---

```

    </defaultValue>
    <constraint nullable="true" />
</string>
<string keyName="Managed Server 6">
    <defaultValue>
        <value></value>
    </defaultValue>
    <constraint nullable="true" />
</string>
<string keyName="Managed Server 7">
    <defaultValue>
        <value></value>
    </defaultValue>
    <constraint nullable="true" />
</string>
<string keyName="Managed Server 8">
    <defaultValue>
        <value></value>
    </defaultValue>
    <constraint nullable="true" />
</string>
<string keyName="Managed Server 9">
    <defaultValue>
        <value></value>
    </defaultValue>
    <constraint nullable="true" />
</string>
</dict>
<presentation defaultLocale="en">
    <fieldGroup>
        <name>
            <language value="en">Mobile Service</language>
        </name>
        <field keyName="Managed Server List" type="list">
            <label>
                <language value="en">Managed Server List</language>
            </label>
            <description>
                <language value="en">Managed Server List</language>
            </description>
        </field>
        <field keyName="Allow Custom Server List" type="checkbox">
            <label>
                <language value="en">Allow Custom Server List</language>
            </label>
            <description>
                <language value="en">Allow Custom Server List</language>
            </description>
        </field>
    </fieldGroup>
</presentation>

```



---

```
<field keyName="Force Passcode" type="checkbox">
  <label>
    <language value="en">Force Passcode</language>
  </label>
  <description>
    <language value="en">Force Passcode</language>
  </description>
</field>
<field keyName="Managed Server 1" type="input">
  <label>
    <language value="en">Managed Server 1</language>
  </label>
  <description>
    <language value="en">Managed Server 1</language>
  </description>
</field>
<field keyName="Managed Server 2" type="input">
  <label>
    <language value="en">Managed Server 2</language>
  </label>
  <description>
    <language value="en">Managed Server 2</language>
  </description>
</field>
<field keyName="Managed Server 3" type="input">
  <label>
    <language value="en">Managed Server 3</language>
  </label>
  <description>
    <language value="en">Managed Server 3</language>
  </description>
</field>
<field keyName="Managed Server 4" type="input">
  <label>
    <language value="en">Managed Server 4</language>
  </label>
  <description>
    <language value="en">Managed Server 4</language>
  </description>
</field>
<field keyName="Managed Server 5" type="input">
  <label>
    <language value="en">Managed Server 5</language>
  </label>
  <description>
    <language value="en">Managed Server 5</language>
  </description>
</field>
<field keyName="Managed Server 6" type="input">
```

---

```
<label>
  <language value="en">Managed Server 6</language>
</label>
<description>
  <language value="en">Managed Server 6</language>
</description>
</field>
<field keyName="Managed Server 7" type="input">
  <label>
    <language value="en">Managed Server 7</language>
  </label>
  <description>
    <language value="en">Managed Server 7</language>
  </description>
</field>
<field keyName="Managed Server 8" type="input">
  <label>
    <language value="en">Managed Server 8</language>
  </label>
  <description>
    <language value="en">Managed Server 8</language>
  </description>
</field>
<field keyName="Managed Server 9" type="input">
  <label>
    <language value="en">Managed Server 9</language>
  </label>
  <description>
    <language value="en">Managed Server 9</language>
  </description>
</field>
</fieldGroup>
</presentation>
<license>anyType</license>
</managedAppConfiguration>
```