

IBM Maximo Mobile 8.11 for EAM  
7.6.1.3

*Installing and configuring Maximo Mobile  
8.11 for EAM*



**Note**

Before using this information and the product it supports, read the information in [“Notices” on page 39.](#)

This edition applies to version 8, release 11, modification 0 of Maximo Mobile for EAM and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright International Business Machines Corporation 2013, 2023.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

- Chapter 1. Introduction to Maximo Mobile..... 1**
- Chapter 2. Product overview..... 3**
- Chapter 3. ... in 8.11..... 5**
- Chapter 4. System architecture..... 7**
- Chapter 5. Installing Maximo Mobile for EAM ..... 9**
  - System requirements ..... 9
  - Installing Maximo Mobile for EAM..... 9
  - Installing the Maximo Mobile for EAM app on mobile devices..... 10
    - Configuring self-signed certificates for the IBM Maximo Asset Management server on iOS devices..... 10
    - Configuring self-signed certificates for IBM Maximo Asset Management on Android devices..... 10
    - Configuring self-signed certificates for the Maximo Mobile Windows application..... 11
  - Setting the URL of the server in the Maximo Mobile for EAM app..... 11
  - Configuring Map Manager..... 12
    - Offline areas..... 14
    - Maximo Application Framework application map tools..... 16
  - Creating a service address with map location..... 17
  - Preloaded data on mobile devices..... 17
    - Creating preloaded data for mobile devices..... 18
  - Refreshing data..... 18
- Chapter 6. Troubleshooting applications on Android..... 21**
- Chapter 7. Configuring Maximo Mobile for EAM..... 23**
  - Configuring authentication ..... 23
  - Defining security privileges for Maximo Mobile role-based applications..... 23
  - Configuring default bar code formats..... 24
  - Configuring properties that affect mobile apps..... 25
  - Recording physical signatures..... 28
  - Configuring an application link..... 29
  - Maximo Mobile REST APIs..... 29
  - Recording e-signature keys..... 31
  - Configuring a mobile device for multiple users..... 33
  - Changing your default insert site in Maximo Mobile ..... 33
- Chapter 8. Maximo Mobile application object structures, query information, and security authorization..... 35**
- Notices..... 39**
  - Trademarks..... 40
  - Terms and conditions for product documentation..... 41
  - IBM Privacy Statement..... 41



# Chapter 1. Introduction to Maximo Mobile for EAM

IBM® Maximo® Asset Management customers can download the Maximo Mobile for EAM app from the Apple App Store or Google Play store.

## Overview of functions

*Table 1. Standard functions*

<b>Function</b>	<b>Description</b>	<b>Availability</b>
Approvals	Approve, assign, and monitor work. This function is only visible to users who have the authority to approve work.	From version 8.3
Defects	Create defects and use artificial intelligence to analyze photos to identify defects. The Defects function is only available to IBM Maximo Civil Infrastructure customers.	From version 8.5
Help & Support	Learn more about how to use the app.	All releases
Inspections	Input results in predefined forms and easily review previous results.	All releases
Inventory Counting	Use count books, ad hoc counts, and reconciliation to ensure valid inventory balances.	From version 8.5
Map	View the locations of your work on a map and plan your route. The map function requires IBM Maximo Spatial to be installed.	All releases
Materials & Tools	See a checklist of the materials and tools that you need to complete your work.	All releases
My Schedule	View detailed information about your work and complete work orders.	All releases
Service Request	Open a service request to report an issue.	From version 8.3
Settings	Specify your preferences for the app.	All releases

Table 1. Standard functions (continued)

Function	Description	Availability
Receiving	Allows the storeroom clerk to receive and stock items from another storeroom within the same organization. Users can look up shipments, scan packages, receive items into inventory, perform inspections, void receipts, and create rotating assets from assets that are received from other sites.	From version 8.10
Issues & Transfers	Storeroom clerks can issue items that are reserved for approved work orders. Users have access to existing inventory usage records from their mobile device.	From version 8.11

### Overview video

Check out the video to learn more about how a technician can complete a work order and an inspection: [IBM Maximo Mobile app overview](#)

### IBM Internet of Things Community

The [IBM Internet of Things Maximo community](#) provides additional information in the form of comprehensive application configuration examples, application upgrade guidance, and other developer resources.

---

## Chapter 2. Product overview

IBM Maximo Mobile for EAM is a next-generation mobile application platform that allows users to securely access IBM Maximo Asset Management functionality from a mobile device.

The Maximo Mobile for EAM Android and iOS apps are available for download from Google Play and the Apple App Store. The Maximo Mobile for EAM Windows app is available on **Passport Advantage Online for Customers**. After a mobile user installs the app on their device and connects to the Maximo Asset Management server, mobile apps that are deployed on the server are set up on the user's device. These apps provide a mobile user with capabilities to manage work and conduct inspections both when the apps are connected and disconnected.





---

# Chapter 3. What's new in Maximo Mobile for EAM

## 8.11

Learn more about what's new and changed in Maximo Mobile for EAM 8.11.

### **Password changes**

If your password is changed on the server, you can log on to the server from your mobile device using the new password. You are then prompted to input your old password to access the local database on your mobile device. If you cancel the prompt for your old password, the existing local database is deleted. Data is then downloaded from the server to create a new local database.

### **Shared device mode**

You can share a mobile device between users without sharing your data.

For more information, see [“Configuring a mobile device for multiple users” on page 33](#).

### **Change default site**

You can change your default site from a mobile device.

For more information, see [Changing the default site](#).

### **Near-field communication (NFC) tag support**

You can use your mobile device to scan asset or location NFC tags to show all the work orders for that asset or location.

### **Mobile Asset Manager enhancements**

Asset Manager includes support for attachments, classify assets in offline mode, view assets in a map, and update specification attributes.

### **Shipment receiving**

Shipment receiving is now available from the Receiving function. It allows the storeroom clerk to receive and stock items from another storeroom within the same organization. Users can look up shipments, scan packages, receive items into inventory, perform inspections, void receipts, and create rotating assets from assets that are received from other sites.

### **Issues and transfers**

Storeroom clerks can issue items that are reserved for approved work orders. Users now have access to existing inventory usage records from their mobile device.

### **FIPS compliance**

Maximo Mobile includes limited support for FIPS 140-2 Validation for Android and iOS platforms.

For more information, see [“System requirements ” on page 9](#).

### **Server selection**

When you log in to a server, you can provide the server address URL by scanning a QR code.

You can also provide the server address by selecting an address from a list of recently used servers.

## Record attachments

Thumbnail images are displayed for image attachments that are listed in the attachment list view for a record.

Multiple records can share an attachment. If one of the records that shares an attachment is removed from the database, the attachment is not removed from the device.

## Service request fields support table domain information

Service request fields now support lookup queries to table domains to specify a field value.

## Electronic audits

Electronic audit records can include Maximo Mobile for EAM data.

Enable e-audit on an attribute for an object that can be edited in a mobile app, for example, the wopriority attribute in the WORKORDER object. When you change the attribute value on a mobile device, the username and timestamp for the change is written to the electronic audit table for the object.

For more information, see [Electronic audit records](#)

## IBM Graphite Declarative Application Framework Developer Reference

The IBM Graphite Declarative Application Framework Developer Reference includes information for Maximo Mobile for EAM developers to develop mobile applications. This reference includes topics on troubleshooting and an API reference.

You can access the guide from the help menu of the Maximo Application Framework Configuration application.

## Maximo Application Framework comment component

A comment component was added to the Maximo Application Framework. You can now add comments in application XML files.

For more information, see [Anatomy of an application XML file](#).

## Maximo Application Framework application upgrade

The Maximo Application Framework Application upgrade automatically captures changes to an application in a delta file that can be applied to the new release of the application. Before Maximo Mobile for EAM 8.11, delta files were updated manually.

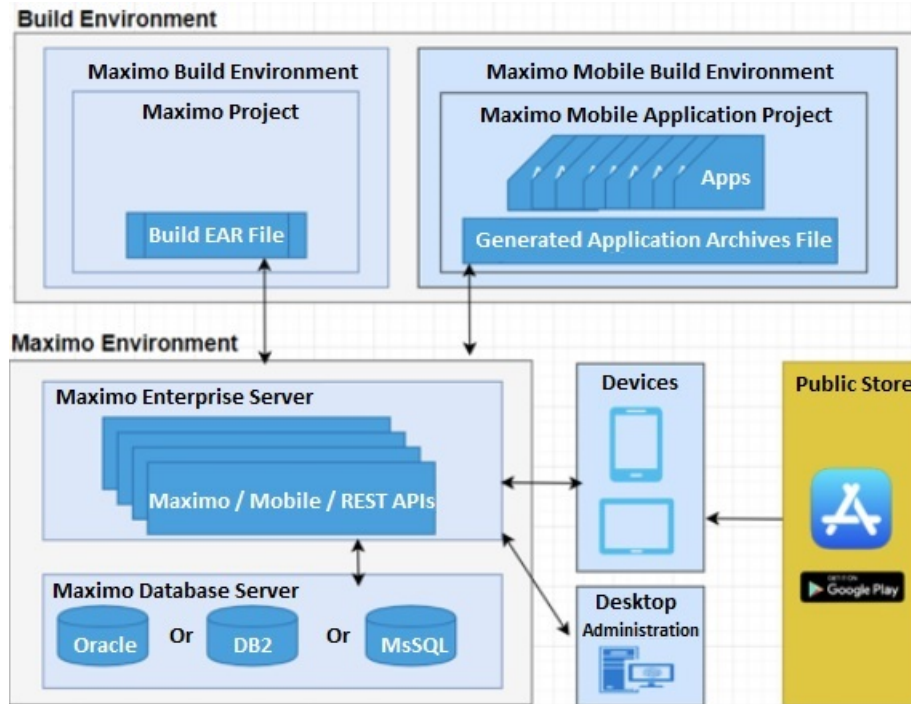
For more information, see [Application upgrade using the Maximo Application Framework Configuration application](#).

## Maximo Application Framework Configuration application canvas improvements

You can right-click components that are rendered in the canvas area of the Maximo Application Framework Configuration application to access a component menu. From this menu, you can cut, copy, paste, and delete components that are displayed in the canvas. When you choose an action, the XML code representing that component in the application XML file updates. For example, if you choose to delete a component from the canvas area, the XML code for that component is deleted from the XML file, including children of that component.

## Chapter 4. System architecture

The following diagram shows the system architecture of Maximo Mobile for EAM and highlights the relationships between key components in Maximo Asset Management:



### Communication and data flow

You can use Maximo Mobile for EAM apps in online and offline scenarios. In an online scenario, the apps are connected to Maximo Asset Management and use the services and data that is provided. In an offline scenario, the apps are not connected to Maximo Asset Management but continue to operate with locally stored data.

When Maximo Mobile for EAM is enabled, inspections are conducted through the Maximo Mobile for EAM user interface. Manage Inspection Forms are located on the Work Center. If Maximo Mobile for EAM is not enabled, inspections are conducted on the Work Center.

### Online and offline operations

When mobile users are online, Maximo Mobile apps interact with Maximo Asset Management and exchange data that is represented in JSON format. In Maximo Asset Management, requests are processed by an OSLC service provider, and a response is returned.

The data that is retrieved from Maximo Asset Management is automatically saved to the local data store on the device. The availability of locally stored data makes online data operations more efficient, and users can continue to work when a planned or unexpected disconnection occurs. While users are online, local data is automatically synchronized to maintain consistency with Maximo Asset Management. Users can also manually synchronize data.

When mobile users are offline, requests are processed on the device by using data that was retrieved during online operations. When connectivity is restored, local data is automatically synchronized. Mobile devices are considered offline when the following conditions are met:

- The device is in airplane mode.

- The network adapter of the device is disabled.
- Network bandwidth is low.
- The Maximo Asset Management is not reachable by the mobile device.
- The login session expires.

Some applications, like Assist and Parts Identifier, require the user to be online.

## Login and authentication

The first time that a user logs in to the Maximo Mobile application, they must have network connectivity, so they can connect to Maximo Asset Management. To log in to the Maximo Mobile for EAM application, the user must enter the credentials that they use in Maximo Asset Management. Using a single sign-on, the user is also authenticated with Maximo Asset Management, and the mobile apps that are on the Maximo Asset Management server are set up on the device. As part of the initial setup, a local JSON data store is created on the device. The data store is a repository for data that is downloaded from the Maximo Asset Management server. The data store is encrypted by using a unique key that is saved in the device's keystore. Each time a user opens the Maximo Mobile for EAM app, they are prompted for their device's security credentials so the application can access the local data store.

When a user authenticates to Maximo Asset Management, they are granted a token, which is used to authenticate all requests to the server. The token lasts for 12 hours after which the user is prompted to authenticate to Maximo Asset Management again. If the user does not authenticate successfully, they work offline until they authenticate to Maximo Asset Management again. A user can authenticate to Maximo Asset Management at any time by clicking the cloud icon from the application screen.

When you successfully use a biometric method to log in to a mobile device and you authenticate with the server through SSO, you have access to your own local database on the device that is used in offline mode. If another user uses biometrics to log in to the same mobile device, but they do not authenticate with the server, they are still able to access data as the last user to authenticate. If the second user was in offline mode, they would access the local database of the first user. The next time the device was used by the second user in online mode, they are given the option to switch users. If they accept, they can now access their own local database when in offline mode.

A user that has access to the device biometrics may access their own local DB after server authentication success. If user does not pass server authentication and he/she is a second user for the app that has access to the device biometrics, he/she would still be able to access as the last user that logged online if they were to access the application offline(they would use the last user's local DB). Then, if he/she logged online, there will be a popup message to let user confirm whether to switch user, if user confirmed, then the app would load current user's local DB. if not, the user would still access the application offline.

For information about security, refer to the [Security](#) topic in the Maximo Asset Management documentation.

---

## Chapter 5. Installing Maximo Mobile for EAM

You can download the server components for Maximo Mobile for EAM from [Passport Advantage Online for Customers](#).

1. Go to the [Passport Advantage Online for Customers](#) website.
2. Sign in with a valid user ID and password.
3. Select IBM Maximo Application Suite Mobile for EAM V8.11.
4. Click **Download Now**.

The downloaded `maximomobileversion.zip` file, contains the following items:

- The Maximo Mobile for EAM apps. When you install Maximo Mobile for EAM, the apps are deployed to Maximo Asset Management. When a user connects to Maximo Asset Management from the Maximo Mobile for EAM app on their mobile device, these apps are set up on the device.
- The desktop applications. A user can access these applications from any browser.
- Maximo Application Framework. The framework provides the environment for the mobile apps to run.
- Scripts to update Maximo Asset Management database tables for Maximo Mobile for EAM.
- A readme file that contains instructions on how to install Maximo Mobile for EAM.

---

### System requirements

Review the system requirements before you install Maximo Mobile for EAM.

Maximo Mobile for EAM must be installed with:

- Maximo Asset Management version 7.6.1.3 or later with IBM WebSphere® Application Server or Oracle WebLogic Server.
- Interim fix IF012 or later for Tivoli®'s process automation engine version 7.6.1.3.
- Interim fix IF010 or later for Maximo Spatial Asset Management version 7.6.1.1.
- Android version 11 or higher, iOS version 14.3 or higher, or Windows 10 version 10.0.17763.0 or better, or Windows 11 operating system installed.

Ensure that your devices and systems are updated with the latest operating system to make sure that you can continue to access the app store.

- Windows devices must include the WebView2 Runtime.

Ensure that you have the latest version of Maximo Mobile for EAM applications available from public mobile app stores or, if you are using Windows, from the IBM portal.

Maximo Mobile for EAM includes limited support for FIPS 140-2 Validation for Android and iOS platforms. The iOS platform relies on [Apple's FIPS certification](#), which is enabled on mobile devices by default. For the Android platform, FIPS validation is enabled by using BoringSSL with FIPS validation enforced. Any Android devices that are certificated with FIPS 140-2 can claim FIPS validation support. Maximo Mobile for EAM supports the TLS 1.3 protocol for the TLS layer. To secure and enforce FIPS compliance, the server or backend API must be configured with TLS 1.3.

---

### Installing Maximo Mobile for EAM

You install Maximo Mobile for EAM on the server where Maximo Asset Management is installed.

To install Maximo Mobile for EAM, follow the installation instructions in the readme file that is included in the `maximomobileversion.zip` file.

After the server-side installation is done and the environment is up, you can access the new role-based applications available with some modules such as Work Order, Inventory and Assets. The Maximo Asset Management system information now lists Maximo Application Framework and Maximo Mobile for EAM.

Test the applications through Maximo Mobile for EAM in a browser before attempting to access them from a mobile device.

## Installing the Maximo Mobile for EAM app on mobile devices

---

For Android and iOS devices, users install the Maximo Mobile for EAM app from Google Play or the Apple App Store. For Windows, you must download the app from [Passport Advantage Online for Customers](#).

To download the Maximo Mobile for EAM for Windows app, complete the following steps:

1. Go to the [Passport Advantage Online for Customers](#) website.
2. Sign in with a valid user ID and password.
3. Select IBM Maximo Application Suite Mobile for EAM Windows App V8.11.
4. Click **Download Now**.
5. Send the app to each mobile user that uses a Windows device to install on the device.

## Configuring self-signed certificates for the IBM Maximo Asset Management server on iOS devices

A self-signed certificate can be installed on the IBM Maximo Asset Management server for iOS devices. The certificate must be imported to each iOS device. This feature is intended for testing and development purposes and not intended for production use. Do not use self-signed certificates for production deployments as they can create a security vulnerability.

1. Download the certificate file.
  - a. Access the IBM Maximo Asset Management server page in your browser on a desktop computer. A message indicates that the connection is not private.
  - b. Find and save the certificate of the root certificate authority. On Safari, click to view the certificate, select the root certificate, and drag the file to a folder.
2. Install the certificate profile.
  - a. Use Airdrop to send the saved root certificate file to your iOS device.
  - b. Open the **Device Settings** page.
  - c. In the User details section of the device settings, click **Profile Downloaded**.
  - d. In the **Install Profile** page, click **Install**.
  - e. If you are prompted, enter the iOS device passcode. A certificate warning is displayed.
  - f. Click **Install** and click **Install** again if you are prompted.
  - g. On the **Profile Installed** page, click **Done**.
3. Trust the certificate.
  - a. On the device, go to **Settings > General > About > Certificate Trust Settings**. The installed root certificate is displayed in the Enable Full Trust for Root Certificates.
  - b. Turn on trust for the certificate that you installed and click **Continue**. The certificate is trusted and enabled and you can proceed to use the Maximo Mobile apps.

## Configuring self-signed certificates for IBM Maximo Asset Management on Android devices

A self-signed certificate can be installed on the IBM Maximo Asset Management server for Android devices. The certificate must be imported on each Android device. This feature is intended for testing

and development purposes and not intended for production use. Do not use self-signed certificates for production deployments as they can create a security vulnerability.

1. Download the certificate file.
  - a. On a desktop computer, in a browser, access the IBM Maximo Asset Management server page. A message indicates that the connection is not private.
  - b. Find and save the certificate of the root certificate authority.
  - c. Copy the certificate file to the Android device.
2. Install the certificate profile on the Android device.
  - a. Open Android settings and then select **Encryption & credentials**.
  - b. Select **Install a certificate** and then select **CA certificate**.
  - c. Select the certificate file that you downloaded.
  - d. After the installation process is complete, select **Trusted credentials** to ensure that the certificate was successfully installed.

## Configuring self-signed certificates for the Maximo Mobile Windows application

A self-signed certificate can be installed on the IBM Maximo Asset Management server for the Maximo Mobile Windows application. This feature is intended for testing and development purposes and not intended for production use. Do not use self-signed certificates for production deployments as they can create a security vulnerability.

1. Export the certificate in Google Chrome.
  - a. On a Windows system, start Google Chrome, and then open the URL for the IBM Maximo Asset Management server.
  - b. In the address bar of the browser, click **Not secure** and then click **Certificate is not valid**.
  - c. In the certificate window, on the **Certification Path** tab, select the first certificate that is listed in the **Certification path** tree and then click **View Certificate**.
  - d. In the new Certificate window, on the **Details** tab, click **Copy to File**.
  - e. In the **Certificate Export Wizard Welcome** panel, click **Next**.
  - f. Select **DER encoded binary X.509(.CER)** and then click **Next**.
  - g. Specify an export file location and then click **Next**.
  - h. When the export process is complete, click **Finish**.
2. Import the certificate to the Trusted Root certificate authorities.
  - a. Right-click the exported certificate file and then select **Install Certificate**.
  - b. In the Certificate Import Wizard panel, select **Local Machine** and then click **Next**.
  - c. Select **Place all certificates in the following store** and then click **Browse**.
  - d. Select **Trusted Root Certification Authorities** and then click **OK**.
  - e. Click **Next** and then click **Finish**.

## Setting the URL of the server in the Maximo Mobile for EAM app

---

To use the Maximo Mobile for EAM app with Maximo Asset Management, the URL of your Maximo Asset Management server must be set in the app. The URL can be set manually by the mobile user or set centrally for each user by using a Mobile Device Management (MDM) application.

Maximo Mobile supports the standard approach to centrally configuring mobile applications that is defined by the [Appconfig Community](#). When you load the Maximo Mobile for EAM Android app in an MDM application, the configurable settings are displayed, and you can set their values. For the Maximo Mobile for EAM iOS app, some MDM applications can load the configurable settings from an `AppConfig.xml`



file. For more information, see the documentation for your MDM application. If your MDM application can load the settings from an `AppConfig.xml`, copy the following configuration details and save to an `AppConfig.xml` file.

```
<managedAppConfiguration>
  <version>1</version>
  <bundleId>com.ibm.iot.maximo.mobile</bundleId>
  <dict>
    <string keyName="serverURL">
    </string>
    <boolean keyName="allowURLtoBeChanged">
      <defaultValue>
        <value>true</value>
      </defaultValue>
    </boolean>
  </dict>
  <presentation defaultLocale="en-US">
    <field keyName="serverURL" type="input">
      <label>
        <language value="en-US">Server URL</language>
      </label>
      <description>
        <language value="en-US"/>
      </description>
    </field>
    <field keyName="allowURLtoBeChanged" type="checkbox">
      <label>
        <language value="en-US">Allow URL to be changed?</language>
      </label>
      <description>
        <language value="en-US"/>
      </description>
    </field>
  </presentation>
</managedAppConfiguration>
```

If your MDM application does not support the `AppConfig.xml` file, you can add the following settings and their values in your MDM application:

Setting	Type	Description
serverURL	String	The URL of the Maximo Application Suite server to which users connect.
allowURLtoBeChanged	Boolean	Allow user to change the server URL in the Maximo Mobile for EAM app. The default value is true, which allows a user to change the URL in the app if, for example, they want to connect to a different server.

If you are not using an MDM application to manage your devices, you must send the URL of the Maximo Asset Management server to each Maximo Mobile user. Each user must then manually enter the URL of the server in the Maximo Mobile for EAM app.

After the URL of the server is set in the Maximo Mobile for EAM app, the Maximo Mobile applications, which are deployed on the Maximo Asset Management server, are set up on the device.

## Configuring Map Manager

Configure Map Manager in an environment with Maximo Spatial Asset Management.

Maximo Spatial Asset Management must be deployed in your environment before you can configure Map Manager.



1. Log in as an administrator. Select your organization from the Organizations application.
2. From the **More Actions** menu, select **Service Address Options**.
3. Select the coordinate option **X and Y** and then click **OK**.
4. Open the Map Manager application, select **New Map Manager**.
5. Configure Map Manager general properties.
  - a) Enter a name and description.
  - b) Select a measurement unit from the **Length and Distance Unit** menu.
  - c) Select **Maximo Spatial** from the **Map provider name** menu.
  - d) Select **Enable map?**.
6. Configure Map Manager map provider properties.
  - a) Set the geographic information system.  
For example,
    - Geocode service URL:  
`https://geocode.arcgis.com/arcgis/rest/services/World/GeocodeServer`
    - Route service URL:  
`https://route.arcgis.com/arcgis/rest/services/World/Route/NAserver/Route_World`
  - b) Add one or more map services:  
For example,
    - **Name:**  
Basemap
    - **URL:**  
`https://basemaps.arcgis.com/arcgis/rest/services/World_Basemap_v2/VectorTileServer`
    - **Order:**  
100
    - **% Transparency:**  
0
    - **Visible:**  
Selected
7. Select the **Services** tab and add services.
  - a) From the Geocode Services section, add a new row.  
For example,
    - **Name:**  
GeoCodeServer
    - **URL:**  
`https://geocode.arcgis.com/arcgis/rest/services/World/GeocodeServer`
    - From Geometry Service section, add the URL. `https://sampleserver6.arcgisonline.com/arcgis/rest/services/Utilities/Geometry/GeometryServer`
    - Click **Save**.
8. Add a new site.
  - a) Select the **Map Manager** tab.
  - b) Click **New Row** and select a site.

- c) Click **Map Initial Extent** and then click **OK**.
  - d) Click **Save**.
9. Configure map tools.
- a) From the **Common Actions** menu, select **Configure Map Tools**.
  - b) Search for Service Address.
  - c) Click **Enable All Map Tools for Selected Application**.
  - d) Click **OK**.

## Offline areas

You can create map areas to use when your mobile device is offline.

You can edit the local map data on your mobile device while it is offline. When connectivity is available, you can synchronize the data with the IBM Maximo Manage server.

## Creating replicas and downloading to mobile devices

You can create a copy of map data for offline mobile devices.

1. Create and configure the map manager record.
  - a) In the Map Manager application, create a new record.
  - b) Choose **Maximo Spatial** for the map provider name, add a site.
  - c) Add and configure map services. Map service layers must be enabled for replicas.
  - d) Save the map manager record and then enable the **Enable Map** option.
  - e) Expand the site that you configured to display the Offline Area Extent section and then add a row.
  - f) Enter an area name and then click **Preview**.
  - g) Zoom in to select the area on the map that you want to replicate for offline use and then click **OK**.
  - h) For each **Map Replica** map service that is listed, click **Create Replica**.  
After the map replica is created, the **Create Replica** button is disabled, and **Delete Replica** button is enabled.
  - i) After the replica is created, click **Create Offline Package**.  
To download the replica to a device, an offline package must be created. An administrator can create an offline package at any time. This package contains all the replicas of that offline area.
  - j) After the offline package is created, the **Package Ready?** option is automatically selected which enables the package for download.
  - k) Select the **Enable Preload?** option to download the replica as preload data to mobile devices.
  - l) Select **Configure Mobile Properties** from the **More Actions** menu and then configure the following properties.
    - pluss.replica.sync.daysToExpire**  
The number of days before an offline map expires. A 0 value indicates that the map never expires.
    - pluss.replica.device.androidPath**  
The folder name that contains the unextracted VTPK file on the mobile device.
    - pluss.replica.device.iosPath**  
The folder name that contains the unextracted VTPK file on the mobile device.
    - pluss.replica.device.windowsPath**  
The folder name that contains the unextracted VTPK file on the mobile device.
  - m) Save the map manager record.
2. Download the offline replica to your mobile device.
  - a) On your mobile device, open the IBM Maximo Mobile application and log in.

- b) Open the mobile application, for example, Technician or Inspections, and then open the map that includes the areas that were selected for the replica.
  - c) Click **Offline Area** and then click **Replicas**.
  - d) Select the replica that you want to download and then tap the download icon.
3. Delete the offline replica from your mobile device.
- a) Open the IBM Maximo Mobile application from your mobile device and log in.
  - b) Open the mobile application, for example, Technician or Inspections, and then open the map that includes the areas that were selected for the replica.
  - c) Click **Offline Area** and then click **Replicas**.
  - d) Select the replica that you want and then click the trash icon to delete the replica.
4. Sync the offline replica on your mobile device.
- a) Open the IBM Maximo Mobile application from your mobile device and log in.
  - b) Open the mobile application, for example, Technician or Inspections, and then open the map that includes the areas that were selected for the replica.
  - c) Click **Offline Area** and then click **Replicas**.
  - d) Select the replica that you want and then click the sync icon to synchronize the replica with the server.

## Creating and downloading vector tile packages












You can create vector tile packages for offline mobile devices.

You must have a .vtpk file available to upload to IBM Maximo Manage. This file that contains map vector tile data and graphic style resources. You can create a .vtpk file with the Package Toolset of the ArcGIS Data Management toolbox. See [Create Vector Tile Package \(Data Management\)](#) for more information.

1. Create the vector tile package.
  - a) In the Map Manager application, create a new record.
  - b) Choose **Maximo Spatial** for the map provider name, add a site.
  - c) Add and configure a basemap.
  - d) Save the map manager record and then enable the **Enable Map** option.
  - e) From the **Common Actions** menu, click **Configure Tile Package**.
  - f) In the **Upload Offline Tile Packages** window, expand the basemap row.
  - g) In the Specify VTPK file section, click **Browse**.
  - h) Select a .vtpk file from your local system and then click **Open**.
  - i) Click **OK**.  
The package file is uploaded to IBM Maximo Manage.
2. Download the .vtpk file to your mobile device.
  - a) On your mobile device, open the IBM Maximo Mobile application and log in.
  - b) Open the Inspections application and then open the map that includes the areas that were selected for the .vtpk file.
  - c) Tap **Offline Area** and then tap **Vector Tile Packages**.
  - d) Select the map that you want and then tap the download icon to download the .vtpk file to your mobile device.

## Maximo Application Framework application map tools

The Maximo Application Framework application toolbar contains all the tools that you use to work with the map.

Tool	Icon	Function
Layers tool		Select map layers to display on the map..
My Location tool		Center the map on the device location.
Home		Center the map on the initial extent view configured in Map Manager.
Identify tool		<p>Identify features on a map.</p> <p>You can also use the Identify tool manage map features.</p> <ul style="list-style-type: none"> <li>• Update the identify tolerance.</li> <li>• Change the highlight color.</li> <li>• Select layers to use with the Identify tool.</li> <li>• Centralize the map on a feature.</li> <li>• Edit and link features.</li> </ul> <p>The Identify tool is enabled by default.</p>
Offline tool		<p>Manage offline resources of the map.</p> <p>You can download, update and delete Vector Tile Package (VTPK) files and layer replicas.</p> <p>The Offline tool is available for mobile devices only.</p>
Indoors tool		<p>Navigate indoor map data, for example, inside a building. You can filter by floors.</p> <p>The Indoors tool is available for webmaps with indoor data capability enabled.</p>
Query tool		Create queries to return a set of map features that match the query criteria. You can use the Query tool to select features on the map.
Edit tool		<p>Can be used to edit or add new features to the map.</p> <p>New features are linked to the current record. You must grant users access to the current service layer from the security application to add or edit features with the Edit tool.</p>
Related tool		Show related work orders for a record.
Results tool		Manage the data retrieved from the Query tool. Use the Results tool to change the status of multiple records through a single server request.
Menu		Open or close the map tools menu.

## Creating a service address with map location

---

Create a service address that includes map location data.

Map manager must be configured with a map provider and map services.

Service addresses can be associated to assets, locations and work orders. A map pin indicates the record location.

1. Log in as an administrator and open the Service address application.
2. Select **New Service Address**.
3. Enter a name, description, and site.
4. Select the **Map** tab.
5. Right-click on any area of the map and select **Set record location**.
6. Click **Save**.

## Preloaded data on mobile devices

---

Instead of downloading individual records to initialize a Maximo Mobile application on mobile devices, you can download a compressed database that contains all supporting data.

### Overview

In previous releases, initializing a Maximo Mobile application for the first time on a mobile device might take an extended amount of time. Downloading applications and storing supporting data from the server to the mobile device took up most of the time that is spent during the onboarding process.

You can now download a prepopulated SQLCipher database that contains all supporting data that is needed by the mobile applications. Each database is customized for a group and delivered as a compressed package to a mobile device.

This database is built on the server regularly by the **MobileDbCronTask** crontask. When applications are updated, the crontask updates the prepopulated database.

### Person groups

Maximo Mobile determines which prepopulated database to download based on assigned person groups. If a user belongs to more than one person group, then they are shown a list of available databases.

When you update a user profile, confirm that the user is a member of the intended group to ensure that they receive the correct database.

### Crontask configuration considerations

How often your data changes dictates how often the **MobileDbCronTask** is run. If your data changes daily, you might consider running the crontask weekly. If your organization establishes new users intermittently, you might consider configuring the crontask to run less frequently. Existing users can always refresh data in their mobile application to ensure that they have the latest information.

### Troubleshooting

If an error occurs during the creation of the SQLCipher database, the log file provides information about the object structure, query, and select statement that generated the error. Returned fields include USERID, SELECT, TABLENAME, SAVEDQUERY, OBJECTSTRUCTURE, and ERRORMESSAGE. The ERRORMESSAGE field contains the error message that is returned by the OSLC integration and the page that generated the error. The administrator receives an email about the crontask failure with log information.

In addition, the administrator can retrieve status information from the browser by opening `HTTPS://hostname:port/maximo/oslc/graphite/mobile/db?info=1&user=username`. The complete

mobile ID record is displayed in JSON for the user who is specified in the **user** parameter. If no user is specified, information for the user who is logged in is displayed. If the **info** parameter is set to **all**, then all of the mobile ID records are returned as JSON.

You can download the entire database as a compressed file to examine its contents. For example, you might want to verify that all expected data is included. Retrieve the database file from the browser by opening `HTTPS://hostname:port/maximo/oslc/graphite/mobile/db?mobileDbId=mobiledbid`. The *mobiledbid* value is included in the JSON information that is displayed for the mobile ID record.

## Creating preloaded data for mobile devices

You can create a preloaded database that contains all supporting data to save mobile application users time when they are onboarding.

Create a cron task that creates the preloaded database that includes the data for all lookup data sources that are defined in Maximo Mobile applications.

1. Log in as an administrator and create a user.

This user is the template user that is used by Maximo Mobile to create the preloaded database. The cron task queries that are used to retrieve the data to load in the database are sent by the template user.

2. Define a default insert site for the user.
3. Assign the user to any standard groups that are used by your organization.
4. Create a person group.
5. Assign the template user as the default user of the new person group.
6. Assign other users to the new person group, so they can receive the preloaded database that is associated with that group.
7. Open the Cron Task Setup application, search for the MobileDbGeneration cron task and then click to configure it.
8. Click **New Row** to create a new instance for the MobileDbGeneration cron task and then name it.
9. Specify the schedule for the cron task, mark it as active, and then enter the template user in the **Run as User** field.

Whenever the cron task runs, the preloaded database is created and stored in the Maximo database.

## Refreshing data

---

You can use the **Data update** page to update the lookup data that is used by Maximo Mobile applications that are running on your mobile device.

The Maximo Mobile navigator consolidates transaction upload and data download tasks. You can refresh several types of data. Transaction data includes a transaction list to upload to the server. Configuration data includes user data and system configuration data. Functions data used to download a compressed file. Record data consists of function data that supports working in offline mode.

1. Open the Maximo Mobile navigator on your mobile device.

2. Refresh data with default updates.

- a) Open the **Data update** screen.

- b) Tap the refresh icon.

Record data is refreshed according to the options that you selected from the **Record data options** screen.

All data is refreshed, including transactions, configurations, functions, and record data.

3. Refresh record data with custom updates.

- a) Open the **Data update** screen.

- b) Tap the **Options** icon.

c) Select the data that you want to update.

Choices include **Supporting data**, **Map data**, **Work list** data, and attachments. If **Work list** data is selected, attachments cannot also be selected. To enable the download of attachments, select the option from the **Offline data** screen from **Settings**.

4. Refresh with all updates of record data.

a) Open the **Settings** screen.

b) Select **Full record update**, and then tap **Update all record data**.

All record data is downloaded.

All functions are placed in a waiting status, and they cannot be accessed until the data download is completed.





---

## Chapter 6. Troubleshooting applications on Android

A debug version of Maximo Mobile for troubleshooting issues is available from IBM Support.

If you encounter issues while using Maximo Mobile, you can contact IBM Support to receive the debug version of Maximo Mobile.

1. Uninstall the release version of Maximo Mobile that you downloaded from the Google Play store.
2. On the mobile device, install the APK file for the debug application.
3. Verify that the **Developer Options** setting is **ON**.
4. Enable USB debugging in **Settings > System > Advanced > Developer Options > USB debugging**.
5. Connect the mobile device to your desktop by using a USB cable.
6. On the desktop, start the Chrome web browser and open the Web Inspector and Debugger tool.
7. Locate the mobile device and application.

Application entries are named **com.ibm.iot.maximo.mobile** or **com.ibm.iot.maximo.mobileeam**.

8. Click **Inspect**.

There are two inspectors available for an application. To inspect Network Requests, use Maximo Mobile Network/DB Inspector. To debug other issues or to inspect the DOM, use the default inspector.

9. Review the collected data.

You can review the data collected to troubleshoot. You can use the debug version for up to 30 days. If you need to continue collecting data, you must reinstall the debug version of the application.



## Chapter 7. Configuring Maximo Mobile for EAM

If Maximo Asset Management uses application server security, you must change the default authentication method that the Maximo Mobile for EAM app uses. After Maximo Mobile for EAM is installed, the mobile apps are ready for use. Depending on your business needs, you can configure certain aspects of the apps.

### Configuring authentication

To log in to the Maximo Mobile for EAM app, users must be authenticated by using the credentials that they use to access Maximo Asset Management. If Maximo Asset Management is configured to use application server security, you must configure the app to use the specific type of authentication that the application server uses.

Application server security supports two types of authentication: form and basic. For more information, see **Configuring user authentication**.

1. In the System Properties application, in the Property name field, enter `maximo.mobile.ldap.isForm`.
2. In the **Global Value** field, enter the value that corresponds to the type of application server security that the Maximo Asset Management server uses. Specify 1 if the server is using form-based authentication or specify 0 if the server is using basic authentication.
3. In the **Common Actions** menu, click **Save Property**.
4. In the Global Properties table, select the checkbox for the property that you set.
5. In the **Common Actions** menu, click **Live Refresh**. The value that you applied to the property takes effect immediately.

### Defining security privileges for Maximo Mobile role-based applications

Maximo Mobile role-based applications such as Technician and Inspections are hybrid applications. These applications can work in a browser, in connected mode or through the mobile application which also supports offline mode. Each mobile application can have one or more settings and object structures that control access to mobile data.

By default, role-based applications do not grant access during installation. Add access to existing security groups. The security for role based applications is made of three parts.

Security component	Overview	Example
Object structure	Role-based applications can rely on Maximo Asset Management and multiple object structures to send data and updates. Role-based applications use OSLC/REST calls to exchange data with Maximo Asset Management. You define the level of access to an object structure from the Object Structure tab of the Maximo Asset Management Security groups application.	When you are editing an asset, the MXAPIVENDOR object can provide a list of vendor companies in the application. READ access is the minimum required to view the list of vendor companies in the role-based application.

Table 4. Maximo Mobile application security components (continued)

Security component	Overview	Example
Object security	Maximo Asset Management does not have an object level security itself. It grants access to object structures which does not ensure that a user has access to the Maximo Asset Management application that owns the object. In the Application security tab of the Maximo Asset Management Security groups application, you can control the level of access to the application and its associated objects.	Maximo Asset Management Companies application must have READ access at minimum to allow the MXAPIVENDOR to access the COMPANIES object.
Application option	Some role-based applications provide the ability to determine what the end user can do. These permissions are determined by the object structure associated with a role-based application. User permissions are defined in the Security options section accessed from the Object Structure tab of the Maximo Asset Management Security groups application.	The Technician role-based application uses the MXAPIWODETAIL object structure. When you select MXAPIWODETAIL from the Object Structure tab, you can control multiple end user features, like status changes, actual reporting and more.

Each application has a security group template. This template gives users the privileges that are needed by each role based application based on the security groups assigned to the user. You can use templates to grant all privileges needed by a role-based application. You can also use templates to view the options available to be configured. You can use the access the Manage/Apply security template option from the Applications tab of the Security Groups application. You can view the application and object structures required by the role-based application. You can grant everyone in a security group access to an application with the Apply Template option.

### Related information

[Creating Work Center and Tool security groups](#)

## Configuring default bar code formats

By default, the bar code reader in the Maximo Mobile for EAM applications tries to read all bar code formats. To reduce the number of formats that the bar code reader tries to read, you must specify one or more default formats that are used in your organization.

Bar code scanning must be performed by using the camera on your mobile device. No other methods are supported. In addition to bar codes, QR codes are also supported.

1. Open the `controller.js` file for each app.
2. Locate the following line in the file:  

```
'mxe.barcode.readers': ['all_formats']
```
3. Change the default value of the property, which is `all_formats`, to the default formats that you want to use. If you want to specify multiple formats, use a comma separator, for example:

```
'mxe.barcode.readers': ['code_128_reader', 'upc_reader']
```

The following bar code formats are supported:

- code\_128\_reader
- ean\_reader
- ean\_8\_reader
- code\_39\_reader
- code\_39\_vin\_reader
- codabar\_reader
- upc\_reader
- upc\_e\_reader
- i2of5\_reader
- 2of5\_reader
- code\_93\_reader

4. Save the `controller.js` file.

5. Optional: In the Technician and Inspections apps, any button that scans bar codes tries to read all of the default bar code formats that you specified. In the `app.xml` for either app, you can override the default bar codes formats that an individual button in the app tries to read.

a. For each app, open the `app.xml` file.

b. Locate the line that contains the button that you want to configure, for example:

```
<barcode-button id="barcodebutton1" on-scan="handleBarcodeScan"
  timeout="30" label="ScanBarcode"/>
```

c. Add the `readers` property to the line and specify one or more bar code formats, for example:

```
<barcode-button id="barcodebutton1" on-scan="handleBarcodeScan"
  timeout="30" label="ScanBarcode"/> readers="{['ean_reader']}" />
```

d. Save the `app.xml` file.

6. Build the apps and deploy them to the Maximo Asset Management server.

## Configuring properties that affect mobile apps

In Maximo Asset Management, you can set system properties that affect the Maximo Mobile for EAM apps.

You configure system properties in the System Properties application in Maximo Asset Management. The following table describes the system properties that you can configure for mobile apps.

<i>Table 5. System properties that affect mobile apps</i>	
<b>Property</b>	<b>Description</b>
<b>mxm.mobile.travel.radius</b>	The radius from the user's GPS location to the work order over which travel time can be tracked. Depending on the user's region, the value is measured in kilometers or miles.
<b>mxm.mobile.travel.prompt</b>	Users can track travel time when the value in <b>mxm.mobile.travel.radius</b> is matched or exceeded. Set to 1 to enable.
<b>mxm.mobile.travel.navigation</b>	In the Maximo Mobile for EAM Technician and Inspections apps, when a user clicks <b>Start travel</b> , a map opens to help the user get to the location of the work. Set to 1 to enable.

Table 5. System properties that affect mobile apps (continued)

Property	Description
<b>mxe.mobile.navigation.ios</b>	<p>When you start a trip, a Maximo Mobile application opens a map service to help you navigate to your destination. Valid values for this property are AppleMaps, GoogleMaps, or Waze.</p> <p>This property requires the <b>mxe.mobile.travel.navigation</b> property to be enabled.</p> <p>Longitude and latitude coordinates are reported. Information about x and y axes is not provided.</p> <p>IOS devices default to using AppleMaps .</p>
<b>mxe.mobile.navigation.android</b>	<p>When you start a trip, a Maximo Mobile application opens a map service to help you navigate to your destination. Valid values for this property are AppleMaps, GoogleMaps, or Waze.</p> <p>This property requires the <b>mxe.mobile.travel.navigation</b> property to be enabled.</p> <p>Longitude and latitude coordinates are reported. Information about x and y axes is not provided.</p> <p>Android devices default to using GoogleMaps .</p>
<b>mxe.mobile.navigation.windows</b>	<p>When you start a trip, a Maximo Mobile application opens a map service to help you navigate to your destination. Valid values for this property are AppleMaps, GoogleMaps, or Waze.</p> <p>This property requires the <b>mxe.mobile.travel.navigation</b> property to be enabled.</p> <p>Longitude and latitude coordinates are reported. Information about x and y axes is not provided.</p> <p>Windows devices default to using GoogleMaps .</p>
<b>maximo.mobile.fetch.timeout</b>	<p>The time in milliseconds that the Maximo Mobile for EAM app waits for a response from the server and also the minimum time that the app stays offline if a response is not received. After the minimum time that the app stays offline expires, the app tries to connect to the server the next time that the mobile user sends a request to the server.</p>

Table 5. System properties that affect mobile apps (continued)

Property	Description
<b>mxe.app.workorder.InspectionBatchRecord</b>	<p>Set to 1 to create batch records for inspections in the same work order, regardless of the hierarchy of the work order.</p> <p>If Maximo Asset Management 7.6.1.2 is installed, but Maximo Mobile for EAM 8.2 is not installed, the <b>mxe.app.workorder.InspectionBatchRecord</b> property does not exist and batch inspections are created by default.</p> <p>If Maximo Asset Management 7.6.1.2 is installed, and Maximo Mobile for EAM 8.2 is also installed, the <b>mxe.app.workorder.InspectionBatchRecord</b> property can be set to 1 to create batch inspections. This property is set to 1 by default.</p>
<b>mxe.app.workorder.StatusToCreateInspection</b>	Defines the internal work order status where the inspection result is created.
<b>mxe.app.inspection.UpdatePendingResults</b>	Set to 1 to update pending inspection results with the newest active revision.
<b>mxe.mobile.inspection.mobilefeatures</b>	Enables features in Maximo Mobile for EAM that are not supported in Conduct an Inspection Work Center.
<b>mxe.mobile.inspection.features.signature</b>	Enables signature input on Inspections forms.
<b>mxe.mobile.inspection.features.multiselect</b>	Enable multiselect input on Inspections forms.
<b>maximo.mobile.usetimer</b>	Specifies whether Start work starts the timer. Set to 0 to change status only and not start the timer.
<b>maximo.mobile.statusforphysicalsignature</b>	The status that requires the user to provide a physical signature.
<b>maximo.mobile.ldap.isForm</b>	This property is used by Maximo Mobile for EAM to detect what LDAP authentication method is used.
<b>maximo.mobile.completetestatus</b>	The status that the work order changes to <b>Complete</b> when work is tapped in Maximo Mobile for EAM.
<b>mxe.webclient.resetMobileSCCache</b>	Reset the mobile start center cache. Resetting the cache might cause portlet loading issues.
<b>maximo.mobile.allowmultipletimers</b>	<p>Determines whether multiple timers can be started at the same time. The default value is <code>true</code>.</p> <p>When set to <code>false</code>, the user can start one timer at a time in Maximo Mobile. Multiple work orders can still have <b>In Progress</b> status. This value applies only for transactions that are started by the user who is logged in to the mobile device.</p>

Table 5. System properties that affect mobile apps (continued)

Property	Description
<b>maximo.mobile.attachments.autoDownload</b>	Automatically downloads files that are attached to a record every time transactional records such as work orders are downloaded or refreshed on a mobile device. You do not need to open each mobile application to download attachments. The default value is true.
<b>maximo.mobile.attachments.filesizelimit</b>	The maximum file size for a file that can be downloaded in the bulk download process. Users can still download the file through the attachment page. The default value is 5120 KB.
<b>maximo.mobile.attachments.zipcount</b>	The increment used to communicate progress of the bulk download of attachments. Progress count is displayed at the interval of the increment. For example, 10 of 100 is displayed, followed by 20 of 100. The default increment display value is 10.
<b>maximo.mobile.attachments.filetypes</b>	Attachment file types available for bulk download. File types include jpg, png, mp4, pdf, doc, xls, and xlst. All file types are included by default.
<b>maximo.mobile.ios.zipdownload.timeout</b>	Dictates the timeout value in milliseconds for IOS native zip file downloads. IOS native zip file downloads include application files, the preloaded database package, and attachments.
<b>maximo.mobile.esignatureenabled</b>	Set to true to enable e-signatures to be used to confirm the status change of a work order in the Technician application.
<b>maximo.mobile.wostatusforesig</b>	Set to a work order status that requires an e-signature. For example, COMP.
<b>mxe.allownativeesig</b>	Set to true to require a native key for Maximo Asset Management instead of user credentials. This property is required to enable e-signatures in Maximo Asset Management.
<b>maximo.mobile.download.parallel</b>	The number of apps that the Navigator can download at the same time. If this parameter is set to 0, all apps are downloaded at the same time. The default value is 3.

Besides these properties, Maximo Mobile for EAM also uses system properties from Maximo Asset Management to determine if SSO is configured and to redirect the user to the SSO login page. Changing these properties in Maximo Asset Management will affect both Maximo Mobile for EAM and Maximo Asset Management. See [Configuring Security Assertion Markup Language \(SAML\) security](#) for more information.

## Recording physical signatures

Maximo Mobile for EAM applications can be configured to require physical signatures for work orders based on their statuses. For example, before a work order is completed, the Technician application can prompt the user to sign the work order and then change its status to complete. This feature is not enabled by default.

You can record and store images of signatures that are submitted from Maximo Mobile for EAM applications. Each signature is stored as an image and as part of an attachment object. The attachment



description is automatically populated with the signature and the date and the time of the signature. A default name is also given to the image, which includes the status of the record it is associated with. After a signature is recorded, it can be retrieved from the attachment list of the signature's associated work order or item.

The signatures can be recorded in both connected and disconnected mode, but the signatures cannot be modified after they are recorded.

1. Log in to Maximo Asset Management and in the System Properties application, open the **maximo.mobile.statusforphysicalsignature** property.
2. Clear the **Nulls Allowed** checkbox.
3. Enter one or more status values in the **Global Value** field.  
For example, enter APPR or COMP.
4. Save the changes.
5. On a mobile device, open the Technician application and then open the details page for a work order.
6. Change the status of the work order to Approved.
7. Write your signature and click **OK**.  
The status of the work order is set to Approved.

## Configuring an application link

---

You can configure an application to open from the field of another application. For example, you can open the Inspections application from a field in the Work Order Tracking application.

1. Log in to Maximo Asset Management and open the Application Designer application.
2. Search for the application you want to modify.  
For example, search for WOTRACK to open the Work Order Tracking application.
3. Select a field in the application.  
For example, select the **Inspection Result** field of the Work Order Tracking application.
4. Open the Properties window for the field.
5. From the **Go To Applications** field, click the magnifying glass icon to open the application search window.
6. Search for a Mobile application.  
For example, INSPECTION.
7. Click the name of the application and then click **OK**.

You can now open the Inspection application from the **Inspection Result** field of the Work Order Tracking application.

## Maximo Mobile REST APIs

---

Maximo Mobile uses REST APIs to download data from Maximo Manage to a user's device.

### Maximo Mobile endpoints

The Maximo Mobile APIs use the following endpoints:

- /maximo/oslc/ping.jsp
- /maximo/oslc/Login
- /maximo/oslc/whoami
- /maximo/oslc/systeminfo
- /maximo/oslc/permission/allowedappoptions
- /maximo/oslc/licenseinfo
- /maximo/oslc/service/system

## Data downloaded by Maximo Mobile APIs

The following table lists the data that is downloaded by the Maximo Mobile APIs for each Maximo Mobile app.

API	Technician app	Approvals App	Inspections App	Service Request app	Inventory Counting
MXAPIDOMAIN	All data	All data	All data	All data	All data
MXAPIALNDOMAIN	All data	All data	All data	All data	All data
MXAPISYNONYMDOMAIN	domainid in ['WOSTATUS','LTTYPE','TIMERS TATUS','ISSUET YP','LINETYPE','ITEMTYPE','ITEMSTATUS','WOC LASS']	domainid in ['WOSTATUS','LTTYPE','TIMERS TATUS','ISSUET YP','LINETYPE','ITEMTYPE','ITEMSTATUS','WOC LASS']	domainid =['INSPRESULT STATUS']	MOBILEDOMAI N	domainid=COU NTBOOKSTATU S
MXAPIFAILURE LIST	FAILUREMOB	FAILUREMOB	No data	No data	No data
MXAPIWODETA IL	ASSIGNEDWOL IST	SUPWOTOAPPR	No data	No data	No data
MXAPIPERSON	No data	No data	No data	All data	No data
MXAPILABOR	LABORSITEMO B	LABORSITEMO B	No data	All data	No data
MXAPILABORC RAFRATE	LABORSITEMO B	LABORSITEMO B	No data	No data	No data
MXAPIINVBAL	ACTIVEITEMSI TE	ACTIVEITEMSI TE	No data	No data	MOBILEINVCN T MOBILEINVCN TREC
MXAPIASSET	SHOWROTATIN GASSET	SHOWROTATIN GASSET	No data	All data	No data
MXAPILOCATIO NS	SHOWLOCATIO NS	SHOWLOCATIO NS	No data	No data	No data
MXAPILOCANC ESTOR	No data	No data	No data	All data	No data
MXAPIOPERLO C	No data	No data	No data	SERVICEREQUE ST ROOTLOCATIO N	All data
MXAPIITEM	SHOWITEMS	SHOWITEMS	No data	No data	No data
MXAPIINVENT ORY	SHOWINVENTO RY	SHOWINVENTO RY	No data	No data	No data
MXAPITOOLITE M	No data	All data	No data	No data	No data

Table 6. Data downloaded by the c APIs (continued)

API	Technician app	Approvals App	Inspections App	Service Request app	Inventory Counting
MXAPIWORKTYPE	All data	All data	No data	No data	No data
PLUSMAPCONFIGURATION	All data	All data	All data	All data	No data
MXAPIINSPECTIONRES	No data	No data	INSPRESULTAL	No data	No data
MXAPIBOOKMARK	No data	No data	No data	SERVICEREQUESTBOOKMARK	No data
MXAPICLASSSTRUCTURE	No data	No data	No data	All data	No data
MXAPICOMPONENT	No data	No data	No data	designcomps	No data
MXAPINOTIFICATION	No data	No data	No data	No data	No data
MXAPIPROP	No data	No data	No data	No data	No data
MXAPISR	No data	No data	No data	SERVICEREQUEST SERVICEREQUESTHISTORY	No data
MXAPISTATEMANAGER	No data	No data	No data	All data	No data
MXAPITKCLASS	No data	No data	No data	SRSUBCATEGORY SRSUBCATEGORYSITE	No data
MXAPITKTEMPLATE	No data	No data	No data	SERVICEREQUEST TKTEMPLATE	No data
MXAPIWORKCENTERFILES	No data	No data	No data	No data	No data
MXAPIWORKLOG	No data	No data	No data	WORKLOGRELATEDOSR	No data
MXAPICNTBOOK	No data	No data	No data	No data	MOBILECNTBOOK
MXAPICNTBOOKLINE	No data	No data	No data	No data	All data

## Recording e-signature keys

Use e-signature keys on your mobile device to confirm that a change is complete and valid.

E-signature keys must be enabled through Maximo Manage system properties before you can use them. Enable the following system settings:

Table 7. Configuring e-signature system properties

Property	Summary
<b>maximo.mobile.esignatureenabled</b>	Set to true to enable e-signatures to be used to confirm the status change of a work order in the Technician application.
<b>maximo.mobile.wostatusforesig</b>	Set to a work order status that requires an e-signature. For example, COMP.
<b>mxe.allownativeesig</b>	Set to true to require a native key for Maximo Asset Management instead of user credentials. This property is required to enable e-signatures in Maximo Asset Management.

Maximo Manage e-signature keys capture and validate work order status changes in the **My Schedule** module of the Technician application. E-signature keys can also be used with applications that are duplicated from the Technician application.

When you change the status of a work order, and you enter an e-signature key on your mobile device, the work order status change transaction is sent to the Maximo Manage server. The e-signature verification request is sent to the Maximo Manage server after the status change transaction completes. If you lose your connection to the Maximo Manage server before the e-signature key is sent, it is sent when you reconnect. Due to many factors, it might take an extended amount of time for the status change transaction to complete.

When it is created, an e-signature key is stored both on the server and the mobile device. When you enter an e-signature key on your mobile device, the Technician application verifies it with the e-signature key that is stored on the Maximo Manage server. If you are using your device in either online or offline mode, the e-signature key is verified against the e-signature that is stored on your device. If your e-signature key is changed on the Maximo Manage server while you are logged in to the mobile device, you must log out and log back in to use the new e-signature key.

You can create an e-signature key from your mobile device during the Maximo Mobile onboarding process. If the Technician application is not installed on your device, you are still prompted for an e-signature if it is enabled on the Maximo Manage server. Alternatively, an e-signature key can be captured and stored on the server in the profile of the user. E-signature keys can be changed on the Maximo Manage server only.

If you log out of Maximo Mobile on your mobile device, then you are prompted for an e-signature key when you next log in. If you refresh data from the Maximo Mobile **Data update** screen, then you are prompted for an e-signature key.

IBM Maximo Asset Management and IBM Maximo Application Suite both require e-signature keys to sign off on work order status changes. When you switch from IBM Maximo Asset Management to IBM Maximo Application Suite, you must enable e-signature system properties, and create an e-signature key in each user profile.

E-signatures keys are not supported in the web version of the Technician application.

Every object and attribute in Maximo Manage can be configured to require an e-signature key. The e-signature key is tracked using the **logintracking** object, validating the change, and associating the user, date, time, the originator record, and the reason for the change.

1. Set e-signature system properties.
2. As a new user, log in to the Technician application with a mobile device.
3. When prompted, set an e-signature key.
  - a) Enter your user ID.
  - b) Enter and verify a new e-signature key.

E-signature keys must include at least one uppercase character, one lowercase character, a number, and a special character such as !, @ #, or \$.

- c) Tap **Save**.

## Configuring a mobile device for multiple users

---

You can share a mobile device between users by enabling the shared device option.

To share a mobile device between multiple users, the device must be in online mode to authenticate the login of a user. When you log out of Maximo Mobile, you have the option to clear all of your data from the mobile device.

1. Open Maximo Mobile from a mobile device.
2. From the **Server address** page, open the **Container settings** page.
3. Enable the **Shared device** option.
4. Return to the **Server address** page and log in to the Maximo Manage server.
5. When you finish your work, you can clear your data from the device by selecting **Clean my data from this device** when you log out.

## Changing your default insert site in Maximo Mobile

---

You can change your default insert site in Maximo Mobile

1. Log in to Maximo Mobile.
2. Tap your user profile.
3. Tap **Default site**.
4. Select a default site from the list.  
You can use the search field to filter the list of available default sites.
5. Tap **Change**.

Your default insert site is updated. You might be prompted to synchronize your data with the server.



# Chapter 8. Maximo Mobile application object structures, query information, and security authorization

Object structures, query information, and related security authorizations that are used in the Technician, Approvals, Inspections, and Service Request applications are listed here. Security authorization assumes that applications are installed by using the same security group.

## Technician and Approvals

Table 8. Technician and Approvals applications object structures, query information, and security authorizations

Object Structure API	Saved Query	Data source WHERE clause	Application page location	Object structure authorizations
<b>mxapisynonymdomain</b>	<b>MOBILEDOMAIN</b>	where="domainid=&quot;ISSUETYP&quot; and maxvalue in [&quot;ISSUE&quot;,&quot;RETURN&quot;]"	Report work	Read
<b>mxapiwodetail</b>	<b>uxtechnicianownerfilter</b>	where="wonum=&quot;{page.params.wonum}&quot; and siteid=&quot;{page.params.siteid}&quot;" where="wonum=&quot;0&quot;"	<ul style="list-style-type: none"> <li>• My Schedule</li> <li>• Work Order</li> </ul>	<ul style="list-style-type: none"> <li>• Read</li> <li>• Save</li> <li>• Insert</li> </ul>
<b>mxapifailurelist</b>	<b>FAILUREMOB</b>			<ul style="list-style-type: none"> <li>• Read</li> <li>• Save</li> <li>• Insert</li> </ul>
<b>mxapiwpeditsetting</b>				Read
<b>mxapiorganization</b>		where="orgid=&quot;{app.client.userInfo.defaultOrg}&quot;"		<ul style="list-style-type: none"> <li>• Read</li> <li>• Save</li> <li>• Insert</li> <li>• Delete</li> </ul>
<b>MXAPIASSET</b>	<b>MOBILEASSET</b>		Report work	<ul style="list-style-type: none"> <li>• Read</li> <li>• Save</li> </ul>
<b>MXAPIOPERLOC</b>	<b>MOBILELOCATION</b>			Read
<b>mxapialandomain</b>				Read

Table 8. Technician and Approvals applications object structures, query information, and security authorizations (continued)

Object Structure API	Saved Query	Data source WHERE clause	Application page location	Object structure authorizations
MXAPIINVENTORY	SHOWINVENTORY		<ul style="list-style-type: none"> <li>Material request</li> <li>Report work</li> </ul>	<ul style="list-style-type: none"> <li>Read</li> <li>Save</li> <li>Insert</li> <li>Delete</li> </ul>
MXAPIITEM	SHOWITEMS		<ul style="list-style-type: none"> <li>Material request</li> <li>Report work</li> </ul>	<ul style="list-style-type: none"> <li>Read</li> <li>Save</li> <li>Insert</li> <li>Delete</li> </ul>
MXAPILOCATIONS	SHOWLOCATIONS		<ul style="list-style-type: none"> <li>Material request</li> <li>Report work</li> </ul>	Read
MXAPITOOLITEM	USERTOOLLIST		Report work	Read
mxapiinvbal	ACTIVEITEMSITE		Report work	<ul style="list-style-type: none"> <li>Read</li> <li>Save</li> <li>Insert</li> <li>Delete</li> </ul>
mxapilaborcraftate	LABORSITEMOB		Report work	Read
mxapilabor	LABORSITEMOB		Report work	Read

## Inspections

Table 9. Inspections application object structures, query information, and security authorizations

Object Structure API	Saved Query	Data source WHERE clause	Application page location	Object structure authorizations
mxapisynonymdomain	MOBILEDOMAIN			Read
mxapiinspections	INSPRESULTALL	where="inspectionresultid={page.params.inspectionresultid}"	<ul style="list-style-type: none"> <li>Main</li> <li>Transition</li> </ul>	Read

## Service Request

Table 10. Service Request application object structures, query information, and security authorizations

Object Structure API	Saved Query	Data source WHERE clause	Application page location	Object structure authorizations
mxapisynonymdomain	MOBILEDOMAIN			



Table 10. Service Request application object structures, query information, and security authorizations (continued)

Object Structure API	Saved Query	Data source WHERE clause	Application page location	Object structure authorizations
mxapiaIndomain				
mxapitktemplate	SERVICEREQUEST TKTEMPLATE		New Request	<ul style="list-style-type: none"> <li>• Read</li> <li>• Save</li> <li>• Insert</li> <li>• Delete</li> </ul>
mxapisr	SERVICEREQUEST	<pre>where="ticketid=&amp;quot; {page.params.ticketid}&amp;quot;";  where="ticketid=&amp;quot;0&amp;quot;";</pre>	<ul style="list-style-type: none"> <li>• My active requests</li> <li>• Service Request</li> <li>• New Request</li> </ul>	<ul style="list-style-type: none"> <li>• Read</li> <li>• Save</li> <li>• Insert</li> <li>• Delete</li> </ul>
MXAPIPERSON	SERVICEREQUEST		New Request	Read
MXAPIOPERLOC	MOBILELOCATION		New Request	Read
MXAPIASSET	MOBILEASSET		New Request	<ul style="list-style-type: none"> <li>• Read</li> <li>• Save</li> </ul>
mxapitkclass	SRSUBCATEGORY		Subcategory	<ul style="list-style-type: none"> <li>• Read</li> <li>• Save</li> <li>• Insert</li> <li>• Delete</li> </ul>



## Notices

---

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
US*

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

*Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, Japan*

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119*

Armonk, NY 10504-1785  
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

#### COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

## Trademarks

---

IBM, the IBM logo, and [ibm.com](http://ibm.com) are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

The registered trademark Linux<sup>®</sup> is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Red Hat<sup>®</sup> and OpenShift<sup>®</sup> are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

Other product and service names might be trademark of IBM or other companies.

## Terms and conditions for product documentation

---

Permissions for the use of these publications are granted subject to the following terms and conditions.

### Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

### Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

### Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

### Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

## IBM Privacy Statement

---

IBM Software products, including software as service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session and persistent cookies that collect each user's name, user name, password, or other personally identifiable information for purposes of session management, authentication, single sign-on configuration or other usage tracking or functional purposes. These cookies can be disabled, but disabling them will also likely eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see the IBM Privacy Statement at <http://www.ibm.com/privacy> in the section entitled “Cookies and Similar Technologies”.





Part Number:

(1P) P/N: