IBM Maximo Mobile 8.8 for EAM
7.6.1.2

Installing and configuring Maximo Mobile 8.8 for EAM

Note

Before using this information and the product it supports, read the information in “Notices” on page 27.

Contents

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

Function	Description	Availability
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	Lean 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 2. Optional functions

Function	Description	Availability
Assist	Get AI insights to increase fix rate and receive remote expert assistance.	All releases

Table 2. Optional functions (continued)		
Function	**Description**	**Availability**
Parts Identifier	Search for and identify industrial parts by using visual and text-based AI.	From version 8.5

Overview video

Check out the video to learn more about how a technician can complete a work order and an inspection:

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.

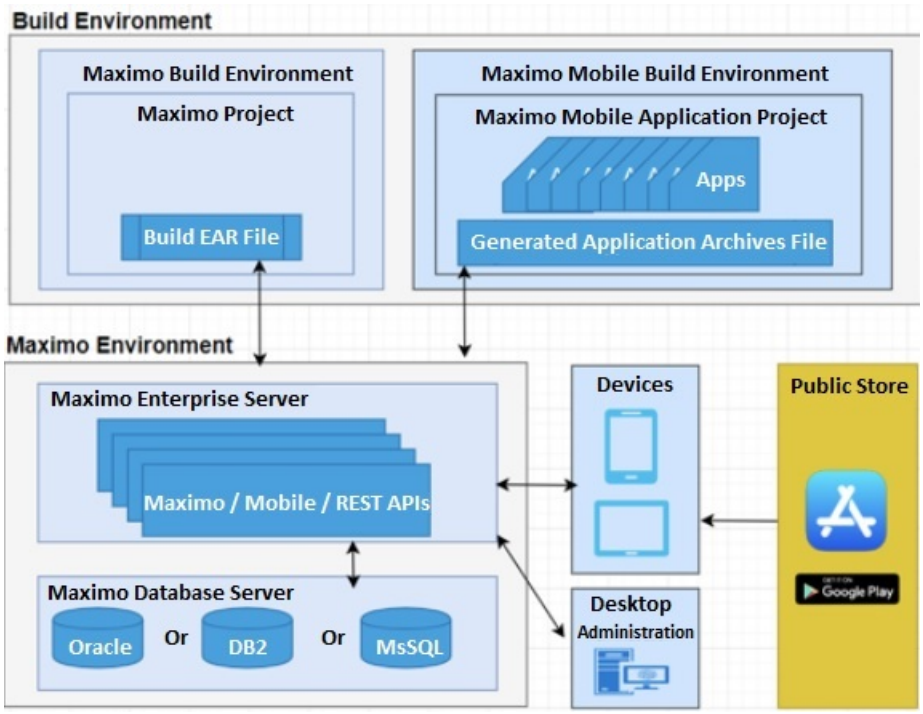
Chapter 2. Product overview

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. 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 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 for EAM 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 device in a JSON data store. 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.

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

Login and authentication

To access remote or locally stored data, users must log in to the Maximo Mobile for EAM app by entering the credentials that they use in Maximo Asset Management. The first time that users log in, they must be connected to Maximo Asset Management. After the first login, depending on connectivity, credentials are validated locally or on the server.

For information about Maximo Mobile for EAM security, refer to the Security. topic in the Maximo Asset Management documentation.

Chapter 4. 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. To download the Maximo Mobile for EAM server components, in the **Part Numbers** field, type `M071YML` and click the search icon.
4. Select IBM Maximo Application Suite Mobile for EAM V8.8 (M071YML).
5. Click **Download Now**.

The downloaded `maximomobile`*`version`*`.zip` file, contains the following items:

- The Maximo Mobile for EAM Technician and Inspections 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 Maximo Mobile for EAM Technician and Inspections 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 7.6.1.2 or later with IBM WebSphere® Application Server or Oracle WebLogic Server.
- Interim fix IF021 or later for Maximo Asset Management version 7.6.1.2.
- Interim fix IF011 or later for Maximo Spatial Asset Management version 7.6.1.
- Android version 10 or 11, iOS version 14.3 , or Windows 10 version 10.0.17763.0 operating system installed.
- Windows devices must include the WebView2 Runtime.
- To use Maximo Mobile for EAM, Android devices must support Ar Core. Refer to ARCore Supported devices for more information.

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 `maximomobile`*`version`*`.zip` file.

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. In the **Part Numbers** field, type M071YML and click the search icon.
4. Select IBM Maximo Application Suite Mobile for EAM Windows App V8.8 (M071YML).
5. Click **Download Now**.
6. 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 Technician and Inspections apps in the Maximo Mobile app.

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:

Table 3. AppConfig settings supported by Maximo Mobile

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:

  `http://geocode.arcgis.com/arcgis/rest/services/World/GeocodeServer`

- Route service URL:

  `http://route.arcgis.com/arcgis/rest/services/World/Route/NAServer/Route_World`

b) Add one or more map services:
For example,

- **Name**:

  `Basemap`

- **URL**:

  `http://server.arcgisonline.com/arcgis/rest/services/World_Topo_Map/MapServer` or `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**:

     `http://geocode.arcgis.com/arcgis/rest/services/World/GeocodeServer`

   - From Geometry Service section, add the URL. `http://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**.

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.

1. On your mobile device, open the **Data update** page.
2. Click the refresh lookup button.
3. On the refresh lookup page, select the refresh button.

A progress bar indicates the status of the download process. By default, only changed or new data is refreshed. All application tiles are placed in a waiting status, and they cannot be accessed until the data download is completed.

Chapter 5. 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.

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 Technician and Inspections 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.

Table 4. System properties that affect mobile apps

Property	Description
mxe.mobile.travel.radius	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.
mxe.mobile.travel.prompt	Users can track travel time when the value in **mxe.mobile.travel.radius** is matched or exceeded. Set to 1 to enable.
mxe.mobile.travel.navigation	In the Maximo Mobile for EAM Technician and Inspections apps, when a user clicks **Start travel**, a map opens to help the user get to the location of the work. Set to 1 to enable.
mxe.mobile.navigation.ios	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`. This property requires the **mxe.mobile.travel.navigation** property to be enabled. Longitude and latitude coordinates are reported. Information about x and y axes is not provided. IOS devices default to using `AppleMaps` .

Table 4. System properties that affect mobile apps (continued)

Property	Description
mxe.mobile.navigation.android	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`. This property requires the **mxe.mobile.travel.navigation** property to be enabled. Longitude and latitude coordinates are reported. Information about x and y axes is not provided. Android devices default to using `GoogleMaps` .
mxe.mobile.navigation.windows	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`. This property requires the **mxe.mobile.travel.navigation** property to be enabled. Longitude and latitude coordinates are reported. Information about x and y axes is not provided. Windows devices default to using `GoogleMaps` .
maximo.mobile.fetch.timeout	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.
mxe.app.workorder.InspectionBatchRecord	Set to 1 to create batch records for inspections in the same work order, regardless of the hierarchy of the work order. If Maximo Asset Management 7.6.1.2 is installed, but Maximo Mobile for EAM 8.2 is not installed, the **mxe.app.workorder.InspectionBatchRecord** property does not exist and batch inspections are created by default. If Maximo Asset Management 7.6.1.2 is installed, and Maximo Mobile for EAM 8.2 is also installed, the **mxe.app.workorder.InspectionBatchRecord** property can be set to 1 to create batch inspections. This property is set to 1 by default.
mxe.app.workorder.StatusToCreateInspection	Defines the internal work order status where the inspection result is created.
mxe.app.inspection.UpdatePendingResults	Set to 1 to update pending inspection results with the newest active revision.

Table 4. System properties that affect mobile apps (continued)	
Property	**Description**
mxe.mobile.inspection.mobilefeatures	Enables features in Maximo Mobile for EAM that are not supported in Conduct an Inspection Work Center.
mxe.mobile.inspection.features.signature	Enables signature input on Inspections forms.
mxe.mobile.inspection.features.multiselect	Enable multiselect input on Inspections forms.
maximo.mobile.usetimer	Specifies whether Start work starts the timer. Set to 0 to change status only and not start the timer.
maximo.mobile.statusforphysicalsignature	The status that requires the user to provide a physical signature.
maximo.mobile.ldap.isForm	This property is used by Maximo Mobile for EAM to detect what LDAP authentication method is used.
maximo.mobile.completestatus	The status that the work order changes to **Complete** when work is tapped in Maximo Mobile for EAM.
mxe.webclient.resetMobileSCCache	Reset the mobile start center cache. Resetting the cache might cause portlet loading issues.
maximo.mobile.allowmultipletimers	Determines whether multiple timers can be started at the same time. The default value is `true`. When set to `false`, the user can start one timer at a time in Maximo Mobile. Multiple work orders can still have **In Progress** status. This value applies only for transactions that are started by the user who is logged in to the mobile device.
maximo.mobile.attachments.bulkDownload.automatically	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`.
maximo.mobile.attachments.bulkdownload.filesizelimit	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.
maximo.mobile.attachments.bulkDownload.zipcount	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`.
maximo.mobile.attachments.bulkdownload.filetypes	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.

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.

Table 5. Data downloaded by the Maximo Mobile APIs

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

Table 5. Data downloaded by the Maximo Mobile APIs (continued)

API	Technician app	Approvals App	Inspections App	Service Request app	Inventory Counting
MXAPISYNONYMDOMAIN	domainid in ['WOSTATUS','LTTYPE','TIMERSTATUS','ISSUETYP','LINETYPE','ITEMTYPE','ITEMSTATUS','WOCLASS']	domainid in ['WOSTATUS','LTTYPE','TIMERSTATUS','ISSUETYP','LINETYPE','ITEMTYPE','ITEMSTATUS','WOCLASS']	domainid =['INSPRESULTSTATUS']	MOBILEDOMAIN	domainid=COUNTBOOKSTATUS
MXAPIFAILURELIST	FAILUREMOB	FAILUREMOB	No data	No data	No data
MXAPIWODETAIL	ASSIGNEDWOLIST	SUPWOTOAPPR	No data	No data	No data
MXAPIPERSON	No data	No data	No data	All data	No data
MXAPILABOR	LABORSITEMOB	LABORSITEMOB	No data	All data	No data
MXAPILABORCRAFTRATE	LABORSITEMOB	LABORSITEMOB	No data	No data	No data
MXAPIINVBAL	ACTIVEITEMSITE	ACTIVEITEMSITE	No data	No data	MOBILEINVCNT MOBILEINVCNTREC
MXAPIASSET	SHOWROTATINGASSET	SHOWROTATINGASSET	No data	All data	No data
MXAPILOCATIONS	SHOWLOCATIONS	SHOWLOCATIONS	No data	No data	No data
MXAPILOCANCESTOR	No data	No data	No data	All data	No data
MXAPIOPERLOC	No data	No data	No data	SERVICEREQUEST ROOTLOCATION	All data
MXAPIITEM	SHOWITEMS	SHOWITEMS	No data	No data	No data
MXAPIINVENTORY	SHOWINVENTORY	SHOWINVENTORY	No data	No data	No data
MXAPITOOLITEM	No data	All data	No data	No data	No data
MXAPIWORKTYPE	All data	All data	No data	No data	No data
PLUSSMAPCONFIGURATION	All data	All data	All data	All data	No data
MXAPIINSPECTIONRES	No data	No data	INSPRESULTALL	No data	No data

Table 5. Data downloaded by the Maximo Mobile APIs (continued)

API	Technician app	Approvals App	Inspections App	Service Request app	Inventory Counting
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	WORKLOGRELATEDTOSR	No data
MXAPICNTBOOK	No data	No data	No data	No data	MOBILECNTBOOK
MXAPICNTBOOKLINE	No data	No data	No data	No data	All data

Chapter 6. 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 6. 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
mxapisynonymdomain	**MOBILEDOMAIN**	`where="domainid=&quot;ISSUETYP&quot; and maxvalue in [&quot;ISSUE&quot;,&quot;RETURN&quot;]"`	Report work	Read
mxapiwodetail	**uxtechnicianownerfilter**	`where="wonum=&quot; {page.params.wonum}&quot; and siteid=&quot; {page.params.siteid}&quot;" where="wonum=&quot;0&quot;"`	• My Schedule • Work Order	• Read • Save • Insert
mxapifailurelist	**FAILUREMOB**			• Read • Save • Insert
mxapiwpeditsetting				Read
mxapiorganization		`where="orgid=&quot; {app.client.userInfo.defaultOrg}&quot;"`		• Read • Save • Insert • Delete
MXAPIASSET	**MOBILEASSET**		Report work	• Read • Save
MXAPIOPERLOC	**MOBILELOCATION**			Read
mxapialndomain				Read

Table 6. 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**		• Material request • Report work	• Read • Save • Insert • Delete
MXAPIITEM	**SHOWITEMS**		• Material request • Report work	• Read • Save • Insert • Delete
MXAPILOCATIONS	**SHOWLOCATIONS**		• Material request • Report work	Read
MXAPITOOLITEM	**USERTOOLLIST**		Report work	Read
mxapiinvbal	**ACTIVEITEMSITE**		Report work	• Read • Save • Insert • Delete
mxapilaborcraftrate	**LABORSITEMOB**		Report work	Read
mxapilabor	**LABORSITEMOB**		Report work	Read

Inspections

Table 7. 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
mxapiinspectionres	**INSPRESULTALL**	`where="inspectionresultid={page.params.inspectionresultid}"`	• Main • Transition	Read

Service Request

Table 8. 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 8. 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
mxapialndomain				
mxapitktemplate	**SERVICEREQUESTTKTEMPLATE**		New Request	• Read • Save • Insert • Delete

mxapisr	**SERVICEREQUEST**	`where="ticketid =&quot; {page.params.ticketid}&quot;"`
		
		`where="ticketid =&quot;0&quot;"`
			• My active requests
			• Service Request
			• New Request
				• Read
				• Save
				• Insert
				• Delete

MXAPIPERSON	**SERVICEREQUEST**		New Request	Read
MXAPIOPERLOC	**MOBILELOCATION**		New Request	Read
MXAPIASSET	**MOBILEASSET**		New Request	• Read • Save
mxapitkclass	**SRSUBCATEGORY**		Subcategory	• Read • Save • Insert • Delete

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.

Each copy or any portion of these sample programs or any derivative work
must include a copyright notice as follows:
© (your company name) (year).
Portions of this code are derived from IBM Corp. Sample Programs.
© Copyright IBM Corp. _enter the year or years_.

Trademarks

IBM, the IBM logo, and 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.

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

The registered trademark Linux® 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.

Other product and service names might be trademarks 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 Online 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.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

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 IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at https://www.ibm.com/privacy/details/us/en/ in the section entitled “Cookies, Web Beacons and Other Technologies”.

Part Number:

(1P) P/N: