WebTMA: On-Premise Mobile WebTMA

TMA distributes Apple iOS/iPadOS and Google Android versions of the WebTMA mobile app for use by clients with on-premise installations of WebTMA.

Distribution

iOS/iPadOS

The iOS/iPadOS app is distributed through Apple Business Manager (ABM). Note that Apple Business Manager and Apple School Manager are interchangeable for the purposes of this document. Your organization must have an ABM account, and you must provide TMA with your ABM organization identifier. Then TMA can make the app available within your ABM instance. Then you can proceed to distribute those licenses either with or without an MDM solution.

Android

The Android version is distributed as a signed binary in both AAB and APK format. TMA will provide you with the actual files for installation, available here.

Configuration

The mobile app supports the following managed app configuration values that can be set through MDM:

Key	`clientUrl`
Type	String
Description	The API base URL for the WebTMA server
Example	`https://example.company.com`
Platform	iOS, Android

clientUrl

- **Purpose**: Specifies the WebTMA server URL that the app will connect to
- **Behavior**: When set via MDM, this value will override any manually entered URL
- **Format**: Must be a valid HTTPS URL pointing to your WebTMA instance
- **Note**: The app monitors for changes to this value and will update automatically

Reference MDM Solution - Microsoft Intune

For reference, we provide basic steps for installing and configuring the WebTMA mobile app in Microsoft Intune. The steps are accurate as of mid-2025. Microsoft Intune may change. The details of your particular MDM solution may differ.

Administrator Setup

Before users can enroll their devices, the IT administrator must complete these steps in Microsoft Intune:

1. **Add Users:**
    - Navigate to Users > All users
    - Click "+ New user" or sync from Active Directory
    - Ensure users have appropriate licenses assigned (Intune or Microsoft 365 license)
2. **Create User Groups (Optional but recommended):**
    - Navigate to Groups > All groups
    - Click "+ New group" to create groups for WebTMA mobile users
    - Add appropriate users to the group
3. **Configure Enrollment Restrictions (Optional):**
    - Navigate to Devices > Enrollment restrictions
    - Set device type restrictions if needed
    - Configure device limit restrictions per user
4. **Set Up Compliance Policies (Recommended):**
    - Navigate to Devices > Compliance policies
    - Create policies for Android and iOS/iPadOS
    - Define minimum OS versions and security requirements
5. **Enable Device Enrollment:**
    - For iOS: Configure Apple MDM Push certificate
    - For Android: Ensure Android enrollment is enabled

Adding Devices

iOS/iPadOS Device Enrollment

To enroll an iOS/iPadOS device in Microsoft Intune:

- Open the App Store
- Search for and install "Microsoft Intune Company Portal"
- Open the Company Portal app
- Sign in with your work account credentials
- Follow the prompts to install the management profile
- Go to Settings > General > VPN & Device Management
- Tap the management profile and select "Trust"
- Return to Company Portal to complete enrollment

Android Device Enrollment

To enroll an Android device in Microsoft Intune:

- Open the Google Play Store
- Search for and install “Microsoft Intune Company Portal”
- Open the Company Portal app
- Sign in with your work account credentials
- Follow the on-screen prompts to complete enrollment
- Accept any required permissions and device management policies

Installing Apps

iOS/iPadOS

Once the iOS/iPadOS device is enrolled in Microsoft Intune and the app is available through Apple Business Manager:

1. **Automatic Installation (Recommended):**
    - In Microsoft Intune admin center:
        i. Navigate to Apps > All apps
        ii. Click “+ Add” and select “iOS/iPadOS store app”
        iii. Search for “WebTMA” in the available apps
        iv. Select the WebTMA app from your Apple Business Manager catalog
        v. Configure app information:
            - Name: WebTMA Mobile
            - Description: WebTMA mobile application for work order management
            - Publisher: TMA Systems
        vi. Set assignment requirements:
            - Minimum OS: iOS/iPadOS 14.0
            - Applicable device types: iPhone, iPad
        vii. Assign to groups:
            - Select “Required” for automatic installation
            - Choose your WebTMA users group
        viii. Review and create the app deployment
2. **User-Initiated Installation:**
    - After app assignment, users can:
        i. Open the Company Portal app on their device
        ii. Navigate to the Apps section
        iii. Find WebTMA in the available apps list
        iv. Tap “Install” to download and install the app
        v. The app will appear on the device home screen once installed

Android

AAB (Android App Bundle)

The AAB format is designed for distribution through Google Play Store or managed app stores:

1. **For MDM Distribution (Recommended):**
    - Upload the `.aab` file to your MDM solution's app catalog
    - In Microsoft Intune:
        i. Navigate to Apps > All apps > + Add
        ii. Select "Line-of-business app" as the app type
        iii. Upload the AAB file
        iv. Configure app information and requirements
        v. Assign to appropriate user groups
2. **For Google Play Console (Private Channel):**
    i. Sign in to Google Play Console
    ii. Create a private app listing
    iii. Upload the AAB file to the release track
    iv. Distribute through your organization's managed Google Play

APK (Android Package)

The APK format allows direct installation on devices:

1. **Direct Installation:**
    - Transfer the `.apk` file to the device via:
        i. Email attachment
        ii. Direct download link
        iii. USB transfer
        iv. File sharing service
2. **Installation Steps:**
    i. On the device, navigate to Settings > Security
    ii. Enable "Unknown sources" or "Install unknown apps" for the file manager or browser
    iii. Locate the downloaded APK file
    iv. Tap to install and follow prompts
    v. After installation, disable "Unknown sources" for security
3. **MDM Distribution:**
    i. Upload the `.apk` file to your MDM solution
    ii. Deploy as a managed app with automatic installation
    iii. No need to enable "Unknown sources" when deployed via MDM

Configuring Apps

To configure the WebTMA mobile app settings in Microsoft Intune:

1. **Navigate to App Configuration:**
    i. Sign in to the Microsoft Endpoint Manager admin center
    ii. Go to Apps > App configuration policies
    iii. Click "+ Add" and select "Managed devices"
2. **Create Configuration Policy:**
    i. **Name:** Enter a descriptive name (e.g., "WebTMA Mobile Configuration")
    ii. **Platform:** Select the platform (Android or iOS/iPadOS)
    iii. **Profile type:** Select "All profile types"
    iv. **Targeted app:** Select the WebTMA mobile app from your app list
3. **Add Configuration Settings:**

    For Android:

    i. In the "Configuration settings" section, select "Use configuration designer"
    ii. Click "Add" to add a configuration key
    iii. **Configuration key:** `clientUrl`
    iv. **Value type:** String
    v. **Configuration value:** Enter your WebTMA server URL (e.g., `https://example.company.com`)

    For iOS/iPadOS:

    i. In the "Configuration settings" section, select "Use configuration designer"
    ii. Click "Add" to add a configuration key
    iii. **Configuration key:** `clientUrl`
    iv. **Value type:** String
    v. **Configuration value:** Enter your WebTMA server URL (e.g., `https://example.company.com`)
4. **Assign the Policy:**
    i. Click "Next" to go to Assignments
    ii. Select the user groups that should receive this configuration
    iii. Under "Required," click "+ Select groups to include"
    iv. Choose your WebTMA mobile users group
        - Click "Next" and then "Create"
5. **Verify Deployment:**
    i. The configuration will be applied when devices sync with Intune
    ii. Users may need to close and reopen the app to see the changes

iii. The configured URL will override any manually entered URL in the app