EMS MOBILE APP Installation Guide

V44.1

Last Updated: August 2018

Table of Contents

CHAPTER 1: Introduction

EMS Mobile App enables easy booking and scheduling on-the-go for mobile devices by enabling you to manage space on mobile devices, such as tablets and smartphones. Simple touchscreen gestures on mobile devices allow you to scan QR codes for rooms and to cancel, end, or check in to meetings.

The EMS Mobile App—which includes the EMS Platform Services—has specific requirements on top of the general EMS server and database requirements. **See Also**: EMS Mobile App System Requirements.

> **NOTE:** You must upgrade to EMS V44.1 (released June 30, 2016) to have the EMS Mobile App. It is not available for earlier versions of EMS.

EMS MOBILE OR EMS MOBILE WEB APP: WHAT'S THE DIFFERENCE?

Although their names are similar and they share the same databases, these products have very different applications.

EMS MOBILE APP = EMS APPLICATION FOR MOBILE DEVICES

This is a separate software application EMS produces specifically to run on mobile devices such as smartphones.

FEATURES OF EMS MOBILE APP THAT ARE NOT IN EMS WEB APP

- Ultra-compact display designed for smartphones
- Two factor authentication method
- QR Code functionality

EMS MOBILE APP = EMS WEB APP ON A MOBILE BROWSER

This is the EMS Web App as it displays when running on a web browser on a mobile device, such as a tablet.

FEATURES OF EMS WEB APP THAT ARE NOT IN EMS MOBILE APP

- Browse Events
- Browse People
- Act As (delegation feature)
- Edit Account Details
- Edit Delegates
- Edit Everyday User Process templates

CHAPTER 2: EMS Mobile App System Requirements

The EMS Mobile App–which includes EMS Platform Services–has specific requirements on top of the general EMS Database Server and EMS Web Server requirements.

> **NOTE:** You must upgrade to EMS V44.1 (released June 30, 2016) to have the EMS Mobile App. It is not available for earlier versions of EMS.

EMS MOBILE APP REQUIREMENTS

SUPPORTED PLATFORMS	
Android	4.4, 5.0, 6.0, 7.0, 7.1
iOS	9.x, 10.x

PREREQUISITES

To host and install EMS Mobile App, you will need the following:

- EMS Database Server

SUPPORTED PLATFORMS
» EMS Web Server
» EMS Platform Services (see also: Licensing Requirements)
» Mobile phone(s)

EMS PLATFORM SERVICES REQUIREMENTS

OPERATING SYSTEM	IIS
Windows Server 2008 R2	8
Windows Server 2012	8
Windows Server 2012 R2	8.5
.NET Framework	4.6.1
Application Pool	4.0
PREREQUISITES	
HTTPPlatformHandler IIS Module	Download Version 1.2 here OR download the installer here.
PowerShell	5+ Version

OPERATING SYSTEM	IIS
ASP.NET Version 4.6	Under Web Server (IIS) > Web Server > Application Development: » ISAPI Extensions » ISAPI Filters » .NET Extensibility 4.6

CHAPTER 3: What's New

DESIGNED FOR EVERYDAY USERS ON THE GO

EMS Mobile App, available on iOS and Android smartphones, is designed primarily for everyday users "on the go." It allows users to make simple reservations in unmanaged spaces (i.e., spaces without services and approvals), such as workspaces and open conference rooms. For example, everyday users may want to:

- Book a meeting space with a few attendees while traveling from their hotel room
- Change the time and/or room for an existing booking
- View where their upcoming meeting is located
- Check-in to or cancel their upcoming meeting

EMS Mobile App uses your phone's hardware features. You can use your phone's camera to scan a QR code to book or check-in to meetings. Administrators can set a proximity-based check-in distance so that users will be able to check-in to their meeting when they are within a certain distance of the building.

Although EMS Mobile App contains many features available on the desktop-browser based EMS Web App, there are some key differences between the two.

EMS MOBILE APP FEATURES NOT IN EMS WEB APP

- Hardware: location, camera
- Offline capability
- Ability to integrate with other mobile apps (e.g., Maps)
- Ultra-compact display designed for smartphones
- Two-factor authentication method
- QR Code functionality
- Proximity-based location search
- Proximity-based check-in validation

EMS WEB APP FEATURES NOT IN EMS MOBILE APP

- Browse events and people
- Act As (delegation feature)
- Edit account details
- Edit delegates
- Edit everyday user process template defaults
- Create / edit service orders

WHAT'S NEW

As of Update 9 (March 2017), EMS Mobile App moved to EMS Platform Services, a middle-tier product that consumes RESTFul API. See Also: Mobile App Release Notes for Update 9.

For more information on enhancements and fixes to the EMS Mobile App, please visit the EMS Release Notes page.

CHAPTER 4: Installation and Basic Setup

This topic provides instructions on how to do the following:

- Install EMS Platform Services on Your Web Server
- Initial Configuration
- Install the EMS Mobile App
- Enable Everyday User Booking Templates

See Also: System Requirements.

INSTALL EMS PLATFORM SERVICES ON YOUR WEB SERVER

1. Log into the EMS Customer Portal.
2. From the **Downloads** dropdown, click the **EMS Software** link.
3. From the **Software and Documents** library, click the **44.1 Releases & Patches** link.

4. Download the **EMSPlatformServices.msi** file and run on your web server.

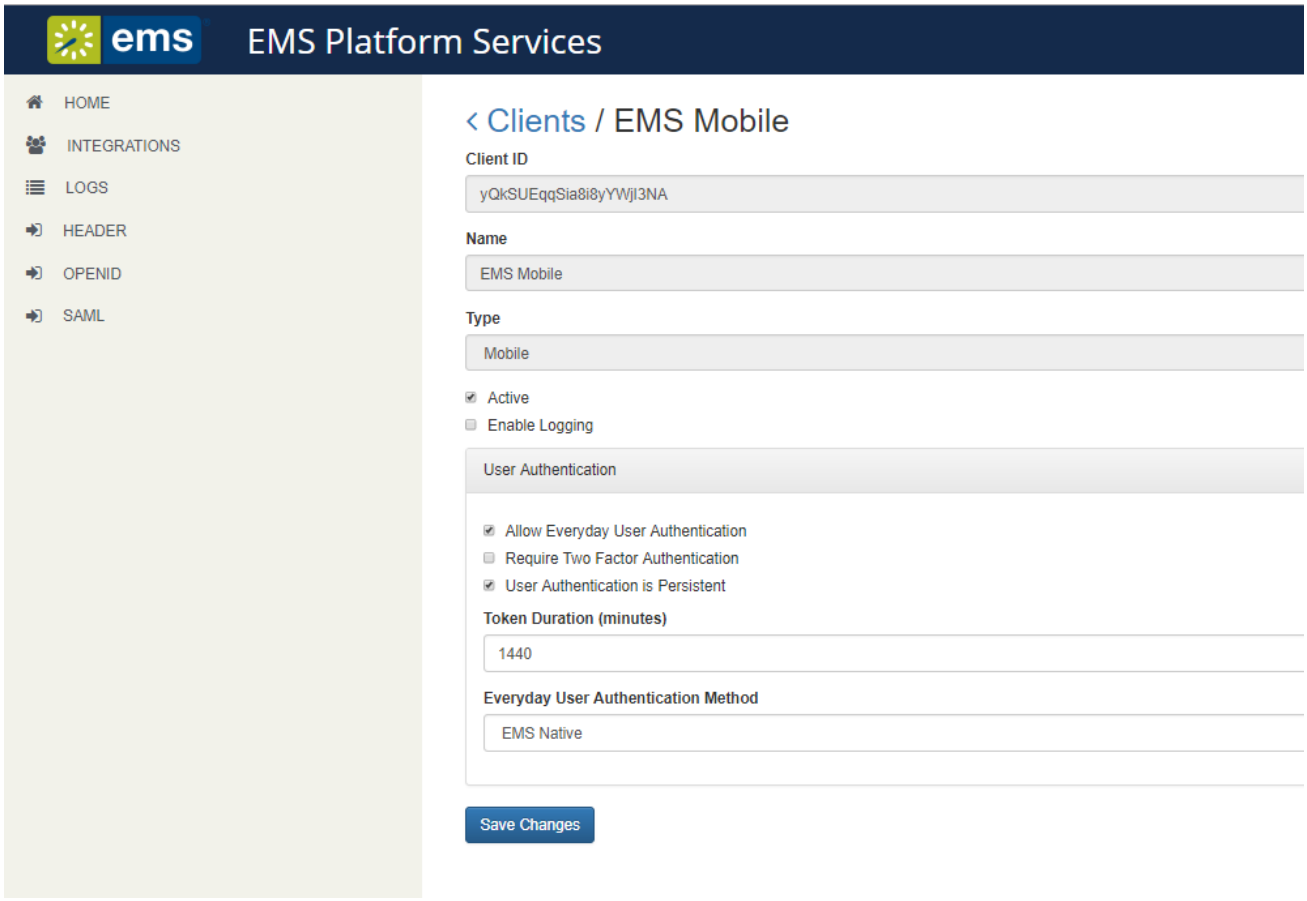
> **NOTE:** You will need to enter the SQL server and EMS database, configured to allow external connections. Make a note of the database name. The typical install path is C:\Inetpub\wwwroot.

5. When all prompts have been completed, click **Install**. The API is now installed on your web server.
6. You will also need a Virtual Directory Name (typical default is **EMSPlatformServices**). Make a note of the new site you have created.

INITIAL CONFIGURATION

1. Access URL for EMS Platform Services (e.g., https://yourcompany.com/ems-platform-api).
2. Log in using your credentials depending on your authentication type. Please refer to configuring Platform Services in the Admin Portal for more details.

3. Click on the **Integrations** tab in the sidebar and select **EMS Mobile.**



4. Select authentication method for everyday users. EMS Mobile App supports the following authentication methods (refer to the guide linked below for guidance in each type of setup):
   - EMS Native Authentication
   - LDAP Authentication

- NTLM Authentication
- Open ID Connect Authentication
- SAML Authentication

> **NOTE:** In addition to the authentications above, EMS Mobile App supports Two-Factor Authentication and Persistent Authentication.

5. Click the "**User authentication is persistent**" box to allow the user to remain logged into the EMS Mobile App. Token duration field determines the duration of persistent login. Default value is 1440 minutes (1 day). This duration can be edited by updating the token duration field.
6. Install the EMS Mobile App (private or public deployment) on user devices and then on each, import the Platform Services URL (based on your user authentication preference). See Also: Deploy the EMS Mobile App.

INSTALL THE EMS MOBILE APP

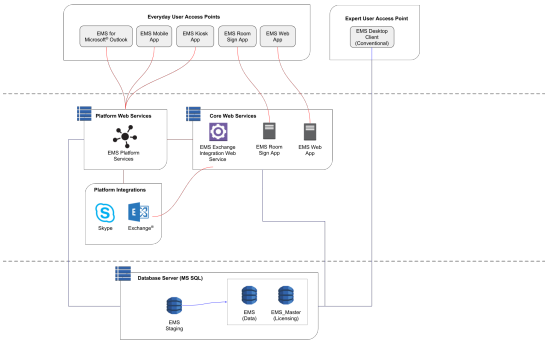
If your organization has EMS Everyday Users licensing, no additional license for EMS Mobile App is required. Your administrator will need to:

1. Download the installation files from the EMS Customer Portal.
2. Ensure that EMS Platform Services is installed and connected to your organization's web server.
3. Configure user authentication.
4. Once these components are in place, users at your organization can add EMS Mobile App to their mobile devices (as a private or public deployment) and enter your server URL and (optional) credentials to authenticate.

CHAPTER 5: Architecture

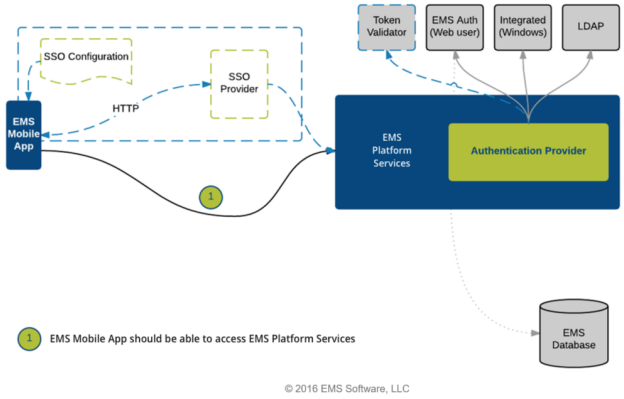
DATA FLOW

The diagram below shows how EMS Everyday Applications interact with EMS Desktop Client, your web and database servers, and Microsoft® Exchange.



AUTHENTICATION

The diagram below shows the authentication process for EMS Mobile App. See Also: Authentication Options.



The EMS Mobile App consists of an iOS or Android native app deployed on users' smartphones, the EMS Mobile App API that sits on a web server, and the EMS database. The EMS Mobile App connects to the API, which authenticates users and talks to the EMS database.

See Also:

- Connect with EMS Platform Services
- How Data Is Stored on Devices

CHAPTER 6: How EMS Mobile App Data Is Stored on Devices

This topic provides information on the following:

DATA AT REST

The following data is likely to be on the device at any given moment during an active user session:

- Per-feature data necessary for the application's functional and business goals:
  - Everyday User data (i.e., information about the current user)
  - Booking and Everyday User Process Template data
  - Favorite Rooms
  - Booking and Room details
  - Other similar feature-related data, subject to change over time

- EMS Platform Services information, including version data and assorted parameter values required for operation
- Application configuration data
- Tokens for authentication:
  - EMS Platform Services token
  - Open ID token(s), if applicable
- Device location information:
  - Location information is stored to speed up certain location calculations that would severely impact performance if the application waited for the underlying OS to return the device's location
- Application logs

Any tokens the application uses are stored in the following areas:

- On iOS, in Keychain
- On Android, in Shared Preferences

ENCRYPTION

The EMS Web App does not currently encrypt any of the data it stores separately from any OS-enforced encryption.

LIFECYCLE

Generally, data stored by EMS Web App remains until the application is uninstalled. Some information may be overwritten during the course of use. For example, if you refresh your bookings for the first time on a given day, yesterday's bookings will no longer be stored by the app. Exceptions include user data that is removed when a user signs out. That data is described below.

SIGN IN

Following is an example response the EMS Platform Services API might send on successful authentication. This constitutes the personal information stored in EMS Web App. Other data stored in the application is information related to that user, but is not information that identifies the user necessarily (i.e., the user's collection of Everyday User Process Templates and bookings, or favorites rooms).

This data is stored every time a user authenticates.

Immediately after successful authentication, EMS Web App sends two requests to the EMS Platform Services API:

1. Download the full body of the user's Everyday User Process Templates for use in creating reservations
2. Verify if the user is or is not a valid user in the configured Microsoft Exchange environment. This data is used to determine whether the user is allowed to create Exchange reservations


```
{
    "userCount": 1,
    "user": {
        "userId": 1234,
        "userName": "test",
        "emailAddress": "test@emssoftware.com",
        "externalReference": "",
        "fax": "",
        "networkId": "",
        "phone": "",
        "timeZoneId": 1,
        "securityState": 0,
        "validated": true,
        "twoFactorState": null,
        "allowAddGroup": true,
        "allowAddContact": true,
        "allowSetDefaultContact": true,
```

```
        "webRoles": [
            {
                "type": 1,
                "code": "eventbrowser",
                "description": "Browse Events"
            }
        ],
        "processTemplates": [
            {
                "id": 1,
                "reserveStatusId": 1,
                "requestStatusId": 2,
                "conflictStatusId": 3,
                "cancelStatusId": 4,
                "allowPersonalization": true,
                "mobileDeviceEnabled": true,
                "webappEnabled": true,
                "outlookEnabled": true
            }
        ],
        "additionalProperties": null
    },
    "trustedDeviceID": null,
```

```
    "webToken": "eyJabc123.def456.ghi789" // example token
}
```

SIGN OUT

When a user signs out of EMS Web App, the following information is deleted from storage:

- Tokens for authentication
- All information received from the EMS Platform Services API indicated in the previous section
  - The user object received during authentication
  - The status of the user in Exchange
  - The user's Everyday User Process Templates
- The current platform API token is also invalidated