EMS Mobile App

Installation, Configuration, & User Guides

April 2019

Accruent, LLC 11500 Alterra Parkway, Suite 110, Austin, TX 78758 www.accruent.com

Table of Contents

CHAPTER 1: EMS Mobile App Installation Guide

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 can:

- 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.

This guide provides information about the following topics:

Contact Customer Support

- **Option 1 (Recommended):** Search the Knowledge Base available at Accruent Access.
- **Option 2:** Submit a case directly via Accruent Access.
- **Option 3:** Email emssupport@accruent.com.
- **Option 4:** Phone (800) 288-4565.

Important!

If you do not have a customer login, register here.

CHAPTER 2: 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 3: What's New

Important!

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.

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 can:

- 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

CHAPTER 4: 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, 8.0
iOS	9.x, 10.x

Prerequisites

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

- EMS Database Server
- EMS Web Server
- EMS Platform Services (See Also: Licensing Requirements)
- Mobile phone(s)

EMS Platform Services Requirements

Operating System	IIS
Windows Server 2012	8
Windows Server 2012 R2	8.5
.NET Framework	4.6.1
Application Pool	4.0

Operating System	IIS
Prerequisites (Prior to Update 28)	
HTTPPlatformHandler IIS Module	Download Version 1.2 here OR download the installer here.
PowerShell	5+ Version
ASP.NET Version 4.6	Under Web Server (IIS) > Web Server > Application Development: • ISAPI Extensions • ISAPI Filters • .NET Extensibility 4.6
Prerequisites (Update 28 and Later)	
ASP.NET Core	See Also: Installing ASP.NET Core.
PowerShell	5+ Version
ASP.NET Version 4.6	Under Web Server (IIS) > Web Server > Application Development: • ISAPI Extensions • ISAPI Filters • .NET Extensibility 4.6

CHAPTER 5: 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

See Also: System Requirements

Install EMS Platform Services on Your Web Server

1. Log into Accruent Access.
2. Click **My Products**.
3. Under **EMS**, click **Downloads**.

   The downloads page opens in a new browser tab.
4. In the **Software Downloads** area, click the link for your version of software, for example, **V44.1 Releases & Patches**.

   A new page opens listing the downloads available based on your license.
5. Download the **EMSPlatformServices.msi** file and run on your web server.

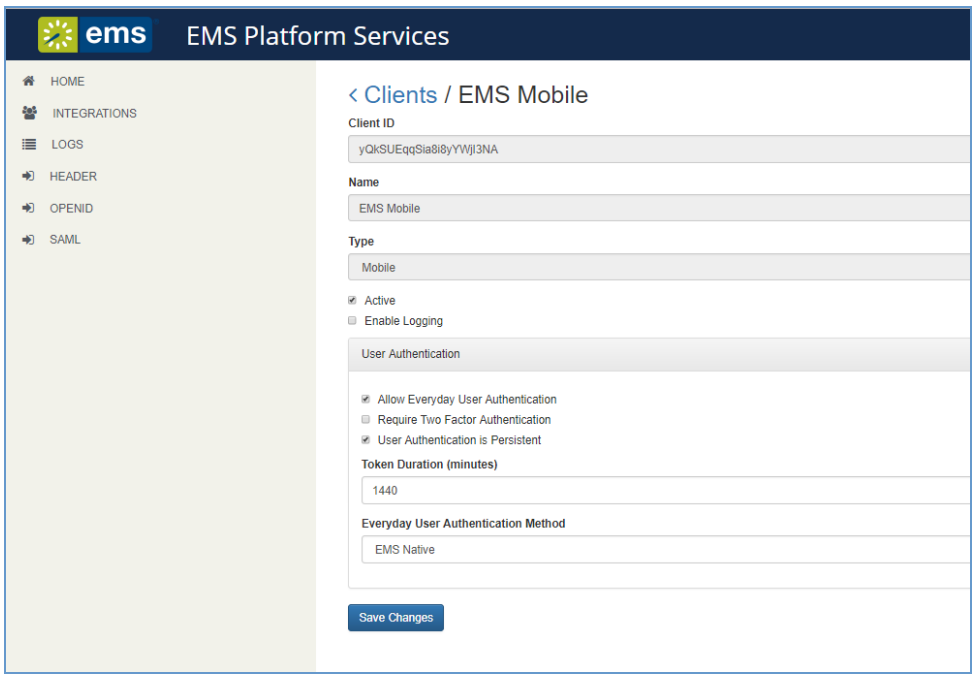
   Note:
   You will need to enter the SQL server and EMS database, configured to allow external connections. Make a note of the database name. The typical install path is C:\Inetpub\wwwroot.
6. When all prompts have been completed, click **Install**. The API is now installed on your web server.
7. You 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/EmsPlatform/admin).
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 Downloads area of Accruent Access.

   To view the Downloads area, log into Accruent Access and click **My Products** > **EMS Downloads** (opens a new tab) > **V44.1 Releases & Patches** (in Software Downloads area).

2. Ensure that EMS Platform Services is installed and connected to your organization's web server.

3. Configure user authentication.

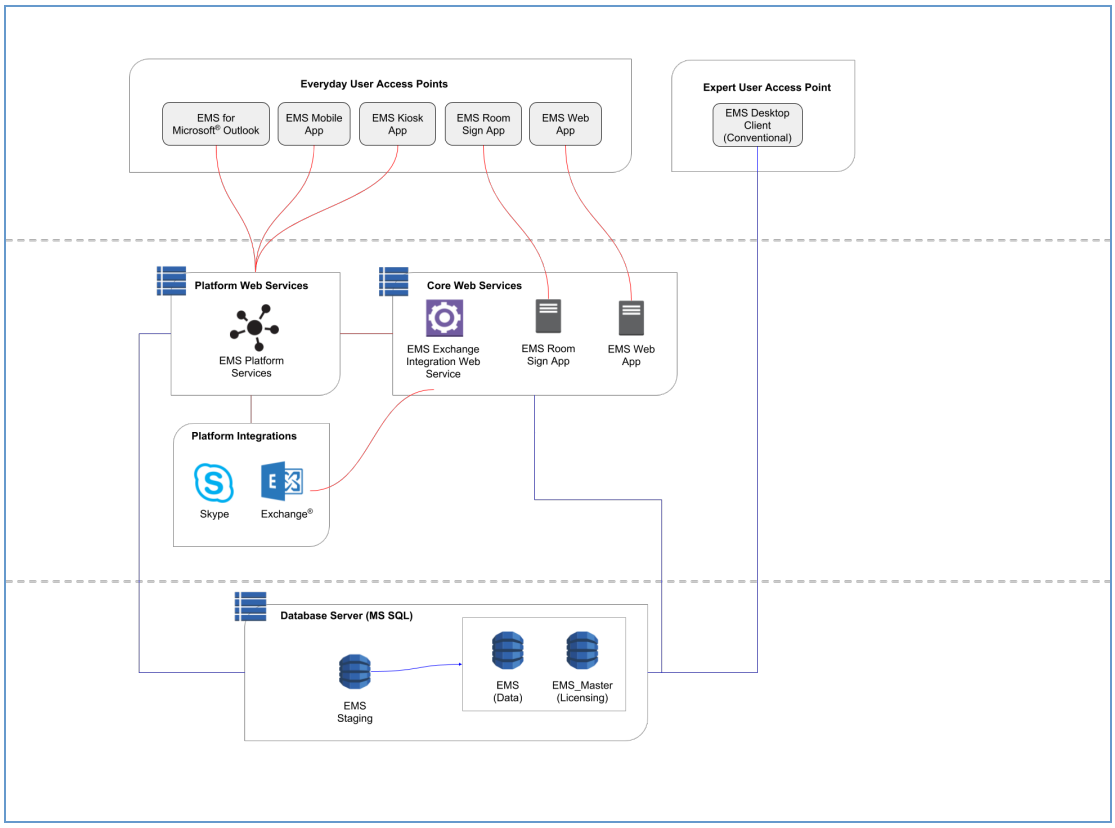
4. Once these components are in place, users at your organization can add EMS Mobile App to their mobile devices (as a private or public deployment) and enter your server URL and (optional) credentials to authenticate.

See Also: Assign Templates to EMS Mobile App Users.

CHAPTER 6: Architecture

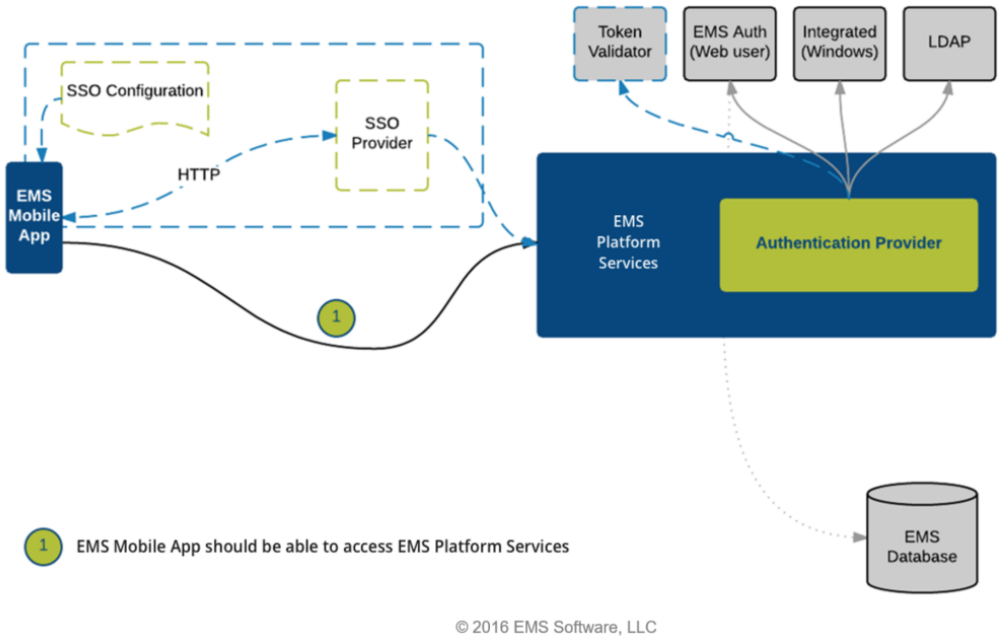
Data Flow

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 7: 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 can 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

CHAPTER 8: EMS Mobile App Configuration Guide

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.

This guide provides the following information for configuring the EMS Mobile App:

Contact Customer Support

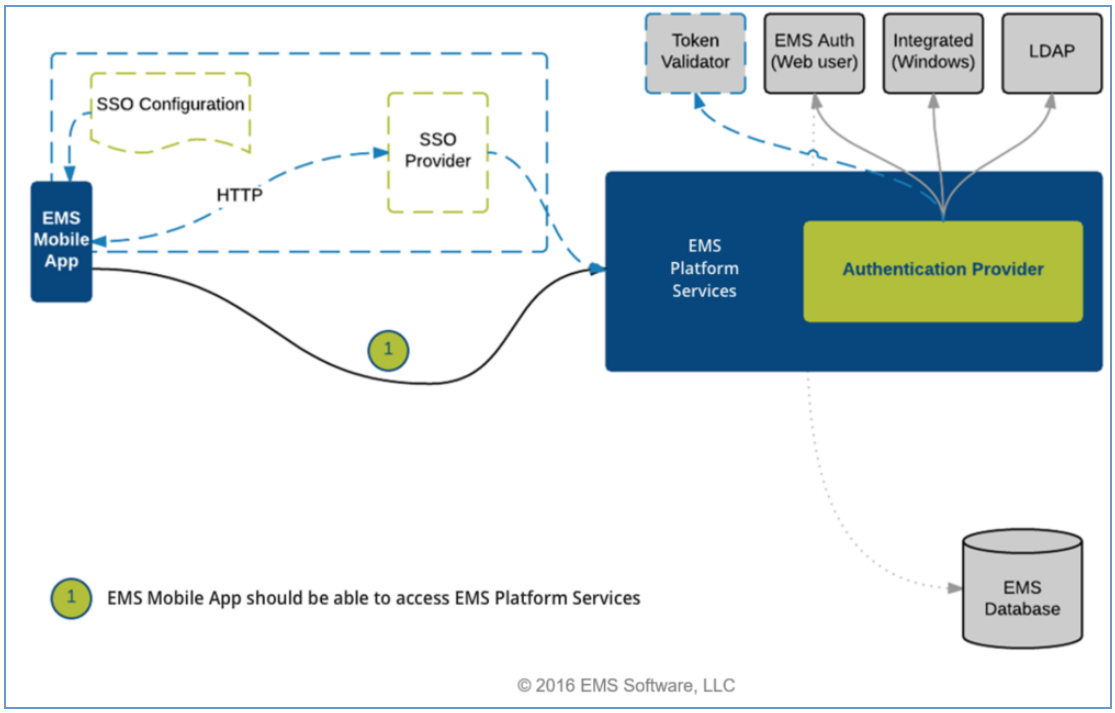
- **Option 1 (Recommended):** Search the Knowledge Base available at Accruent Access.
- **Option 2:** Submit a case directly via Accruent Access.
- **Option 3:** Email emssupport@accruent.com.
- **Option 4:** Phone (800) 288-4565.

Important!

If you do not have a customer login, register here.

CHAPTER 9: Configure EMS Mobile Authentication

This section provides the following information about configuring EMS Mobile Authentication.



Authentication options for the EMS Mobile App include:

- EMS Native Authentication
- LDAP Authentication
- Open ID Connect Authentication
  - Open ID Connect Authentication Can Be Hosted or Pre-Configured in the EMS Mobile App
- Persistent Authentication
- SAML Authentication
  - SAML Authentication Can Be Hosted or Pre-Configured in the EMS Mobile App
- Windows Authentication (NTLM) for EMS Mobile

CHAPTER 10: SAML Authentication

This section guides you authenticating your users with a SAML provider. Authentication with SAML requires configuration prior to beginning the authentication flow.

This topic will give you information on the following:

Prerequisites

EMS Platform Services is required for SAML authentication.

EMS Web App

The minimum version of EMS Web App and EMS Platform Services for authentication through SAML 2.0 is Update 23.

Note:

For EMS Web App, Administrators must enable SAML 2.0 authentication by changing the following parameter value to **Yes** in EMS Desktop Client:

1. Navigate to **System Administration** > **Settings** > **Parameters** > **Everyday User Applications** tab > **Authentication** > **Use SAML 2.0 Authentication for User Authentication Web App Only**.
2. Select YES.

If set to **No**, EMS Web App will utilize SAML as configured through Portal Authentication methods.

EMS Mobile App

The minimum version of EMS Platform Services for SAML authentication in the EMS Mobile App is Update 9. There are breaking changes in Update 23 and customers will be required to update SAML configuration

settings.

Supported Identity Providers

- ADFS
- G Suite
- Okta
- Auth0
- Azure AD
- Shibboleth

> **Note:**
> Only Redirect HTTP Binding Type is currently supported.

Update SAML configuration

1. Delete existing identity and service provider keys. As of Update 23 (March 2018), SP and IdP certs are stored in the database instead of the file system of EMS Platform Services.
2. Generate encryption key.
3. Update SAML configuration based on these settings.

Configure SAML Authentication for EMS Mobile App and EMS Web App

Prerequisite

Update the Encryption key in default.Json file.

> **Note:**
> The Encryption Key is used for encrypting and decrypting the Service Provider private key when stored in the database via the AuthKey API.

New Customers: The encryption key is already provided in the default.json file.

Existing Customers: The encryption key needs to be generated and added to the default.json file before using the AuthKey API. Run the following command in a terminal, openssl rand -Base64 32, to generate a 256-bit key that is Base64 encoded. The encryption key must be 256-bit and must be Base64 encoded. Restart EMS Platform Services after updating default.Json file.

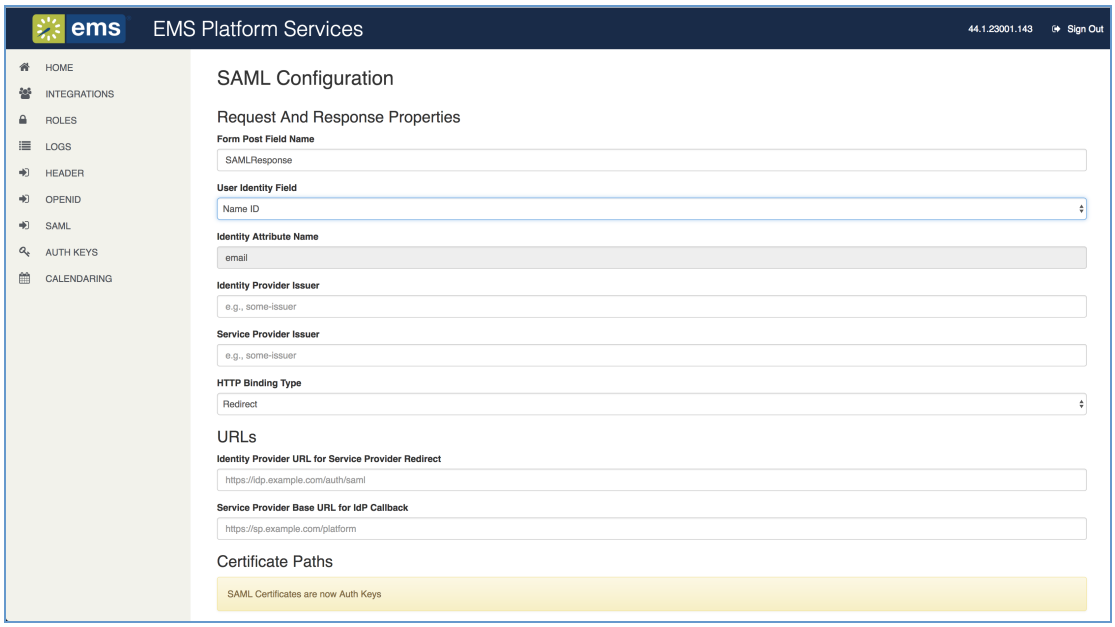
1. Login to EMS Platform Services.
2. Navigate to the Integrations tab.
3. Select EMS Mobile / EMS Web Application.
4. Set **Everyday User Authentication Method** to **SAML** and save changes.
5. Select SAML from the left navigation bar.
6. Configure SAML authentication settings.

> **Note:**
> SAML settings are global and will apply to all integrations utilizing SAML authentication.

Identify Your Provider in Configuration

You are responsible for the configuration of your chosen IdP, with information relevant to the EMS Platform Services acting as a Service Provider for SAML Authentication. The following EMS Platform Services related settings might be needed in order to configure your IdP.

The following fields are required to complete SAML authentication configuration:



Field	Description
Request and Response Properties	
Form Post Field Name	(Optional, default is SamlResponse). Attribute in which assertions are sent, within encoded <samlp:Response> document.

Field	Description
User Identity Field	**REQUIRED**. Drop-down list with choice of assertion element containing user identity (Name ID or Attribute). If set to Attribute, then you must set the Identity Attribute Name to the expected assertion attribute name to use for user identity.
Identity Attribute Name	Assertion attribute name containing user identity. Attribute names can be identity provider-specific (i.e., 'uid', 'mail'). This field is ignored when User Identity Field is set to Name ID.
Identity Provider Issuer	**REQUIRED**. Used to verify expected issuer of assertions, included in SAMLResponse as <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion" >http://adfs.mycompany.net/adfs/services/trust</Issuer>.
Service Provider Issuer	**REQUIRED**. Included by EMS Platform Services in AuthnRequest requests sent to Identify Provider. This is included in the SAMLRequest as <saml:Issuer>https://mycompany.com/EmsPlatform</saml:Issuer> EMS Platform Services will autogenerate the values for the Service Provider Issuer and the Service Provider Base URL for IdP Callback.
HTTP Binding Type	Specifies which SAML binding (HTTP Post or HTTP Redirect) EMS Platform Services will use to transmit SAML protocol messages. **Currently only Redirect is supported.**
URLs	
Identity Provider URL for Service Provider Redirect	**REQUIRED**. This URL, (e.g., https://idp.example.org/SAML2/SSO/Redirect), includes the authentication request details provided by EMS Platform Services and contains opaque data that it includes in the request. This enables the Identify Provider to include it as Relay State on the SAMLResponse. **Note:** If you have the identity provider metadata.xml file, you can upload it through the EMS Platform Services endpoint https://company.platform/api/v1/authentication/saml/metadata/idp. The identity provider certificate will be uploaded for you and Identity Provider Issuer. The Identity Provider URL for Service Provider Redirect fields will be populated for you.
Service Provider Base URL for IdP	**REQUIRED**. Set this URL to the base URL of the EMS Platform Services installation

Field	Description
Callback	(i.e., https://mycompany.com/EmsPlatform). EMS Platform Services will autogenerate the values for the Service Provider Issuer and the Service Provider Base URL for IdP Callback.
Certificate Paths	
	Important! SAML Certificates are now Auth Keys. These fields are not editable.
Path to Identity Provider Public Certificate	**REQUIRED**. Uploaded through Auth Keys.
Path to Service Provider Public Certificate	Optional. Uploaded through Auth Keys.
Path to Service Provider Private Certificate	Optional. Uploaded through Auth Keys.

How EMS Platform Services Supports SAML

No Two-Factor Authentication (2fa) support is provided with SAML authentication. 2fa is the responsibility of the Identity Provider (3rd-Party or Customer owned) and not the EMS Platform Services. Token expiration is configured and managed the same for SAML as for other authorization types, thus overriding any SAML Assertion Conditions that specify the assertion expiration timestamp.

Note:

See Also: Persistent Authentication for token expiration configuration details. Refer to Customize Your Mobile App Configuration Using config.json for details on building a configuration file for EMS Mobile App.

Once you have created your configuration file, you can proceed with one of the sections below, depending on whether you intend to host the file or pre-configure the application and redistribute it.

Using Hosted Configuration (Public Deployment)

Host your configuration file from an applicable web server. Distribute the URL to your end users.

Important!

It is not recommended to make this configuration file publicly available, since it will likely have URLs and/or other information in it that you do not want made available. Instead, host the file in a way such that it is only available internally to your organization. Users should only have to perform this import one time per installation of the application.

Pre-Configure EMS Mobile App (Private Deployment)

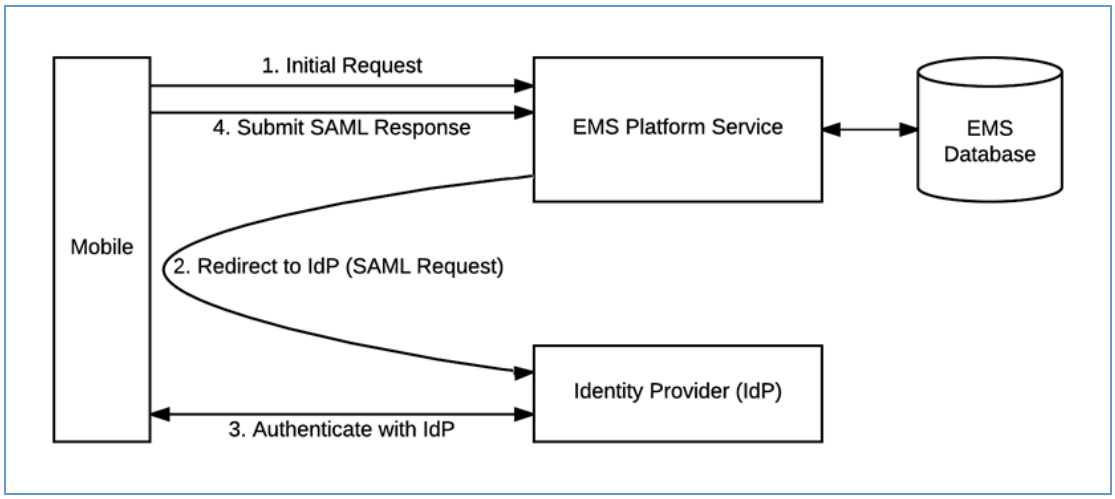
If you want to pre-configure EMS Mobile App, see Configure and Re-Sign the EMS Mobile App.

CHAPTER 11: SAML Authentication Can Be Hosted or Pre-Configured in the EMS Mobile App

Hosted Configuration: The configuration can be hosted at a URL available to end users. The user will then enter that URL into the application. EMS Mobile App will download and use that information, and kick off the authentication process. When configured this way, users will launch the EMS Mobile App and see the EMS Server URL screen. Instead of entering an EMS Server URL, the user will tap **About** near the bottom right of the screen and select the option to **Import SSO Configuration**. The user will then tap **Import** Mobile app, which will direct the user to enter the **Configuration URL**. Then the user will tap **Import**.

Pre-Configured In EMS Mobile App: The configuration can be "baked" into the application. This requires re-signing, hosting, and re-distributing the EMS Mobile App within your organization. With a pre-configured EMS Mobile App users do not need to import any SAML configuration details. EMS Mobile App will launch with that configuration and use it directly.

How Users Authenticate After Configuration



EMS Mobile App makes a request to the configured or default SAML URL

- If the request redirects the user to the SAML authentication web page, then the web user will see the page in a web view inside EMS Mobile App.
- The user might briefly see a busy indicator while the page loads.

Users will authenticate using the SAML authorization view. They do not participate in the steps that follow. They may, however, see the screen change during this process. Successful authentication will send an HTML response back to EMS Mobile App, which will silently POST the SAML form and response to the EMS Platform Services API. EMS Platform Services API will then parse the SAML response and find the

corresponding user in the EMS database. Then EMS Platform Services API will respond to EMS Mobile App, which will direct the user to the Home screen. If the EMS Platform Services API is unable to verify the credentials, EMS Mobile App will present an error message informing the user.

How the Identity Provider (IdP) Works

The Identity Provider (IdP) handles the input and verification of end user credentials. It also issues and verifies tokens. The EMS Mobile App must be registered with the IdP. The client_id generated by this registration is required information for the configuration used by the EMS Mobile App and the SAML flow.

How the EMS Platform Services API Works

The EMS Platform Services API receives the access_token from the EMS Mobile App. The token is then sent to the userinfo endpoint for verification. The response from the userinfoendpoint is used to find a user in the EMS database. The API will then respond to the EMS Mobile App based on the results of this process.

CHAPTER 12: NTLM Windows Authentication

Follow the steps in this section to authenticate your users with Windows Authentication via Microsoft's NTLM challenge-response protocol.

> **Note:**
> Windows Authentication requires that you install and use the optional EMS Platform Services API.

User Login Scenario

Once you have established a connection to the EMS Platform Services API, the user log-in process is as follows:

- Users will enter domain credentials to log into their EMS product.
- EMS will send credentials to the EMS Platform Services API.
- IIS will intercept the call and issue a challenge.
  - The EMS access point (e.g., EMS Mobile App, EMS Web App, etc.) will then perform all steps necessary to complete process with the user's provided credentials.
- EMS Platform Services API receives the initial request and extract the authenticated user from the IIS context.
- EMS Platform Services API will verify the authenticated user against the EMS database.
- User will be taken to the **Home** screen.

If the credentials are missing when the user taps **Sign In**, an error message will appear indicating that fields are required. If the EMS Platform Services API is unable to verify the authenticated user, or if IIS rejects the request due to failed authentication, EMS will inform the user.

Test Your Windows Authentication

Assuming you have installed the EMS Platform Services API at https://Yourcompany.com/EmsPlatform, then you can test the authentication with a curl command:

```
curl -X POST -H "x-ems-consumer: MobileApp" -H "Content-Type: application/json" --ntlm  -u your_username:your_password -vvvv -d '{}'  "https://ems.yourcompany.com/endpoint...authentication"
```

...where your_*username* and your_*password* are your credentials.

> **Note:**
> **api/v1/authentication** is the endpoint within the API where your request must be sent.

CHAPTER 13: LDAP Authentication

Lightweight Directory Access Protocol (LDAP) is an application protocol for querying directory information. The LDAP Authentication method provides single-sign-on capability using your organization's LDAP environment and can be used in both intranet and internet deployments of EMS Everyday applications such as EMS Web App and EMS Mobile App.

For example, when a user logs into EMS Web App or EMS Mobile App with their User ID and Password, their credentials are authenticated against LDAP and compared against corresponding user information recorded in the Network ID and/or External Reference fields of your EMS Everyday User records. If a match exists, the Everyday User will be logged in to the application, inheriting any Everyday User Process Template rights to which their LDAP Group has been assigned.

Note:

The EMS Web App LDAP-Process Template assignment process requires that your implementation of LDAP stores group information (e.g., staff, student, department, etc.) as a Directory Service object containing a property (i.e., member) that contains the users that belong to your various groups.

Note:

The Field Used to Authenticate Everyday User parameter (within System Administration > Settings > Parameters (Everyday User Applications tab) is used by the applications to determine which value should be used for authentication.

Follow the steps in this section to authenticate your users via LDAP. After successful connection to the platform API, the user will log in following the scenario below:

- The user will enter credentials on the Sign In screen and tap **Sign In**.
- EMS Mobile App will send credentials to the EMS Platform Services.
- EMS Platform Services will verify credentials against the configured LDAP provider.
- EMS Platform Services will respond to the EMS Mobile App.
- User will be taken to the Home screen.

If the credentials are missing when the user taps **Sign In**, an error message will display stating that fields are required. If the platform API is unable to verify the credentials, the mobile app will inform the user based on that response.

To use LDAP authentication, you will need to:

1. Configure your LDAP Provider.
2. Test your LDAP Configuration.

3. Test your LDAP Authentication.

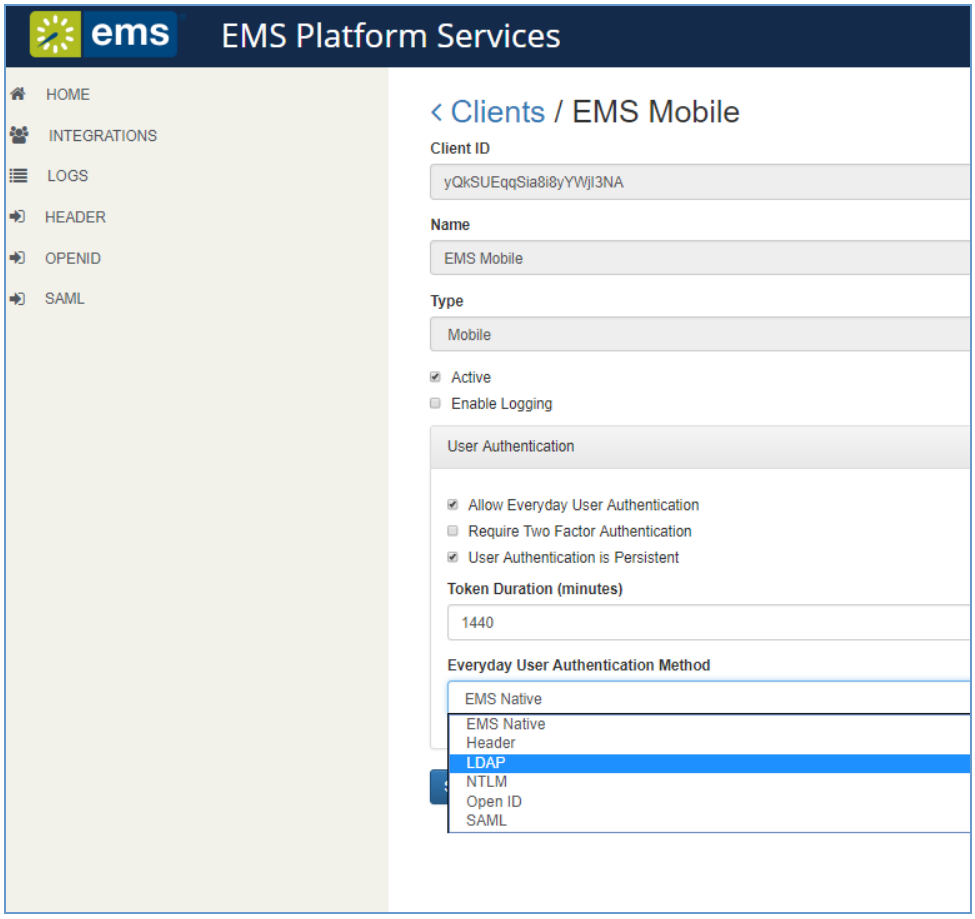
This topic covers the following topics related to LDAP configuration:

- Configure EMS Web App to Use LDAP Authentication
- Configure EMS Web App Security
- Configure Communication Options
- Core Properties
- Non-AD Config
- LDAP Queries
- Save Your Configuration
- Test Your Configuration
- Configure Authentication for EMS Mobile App

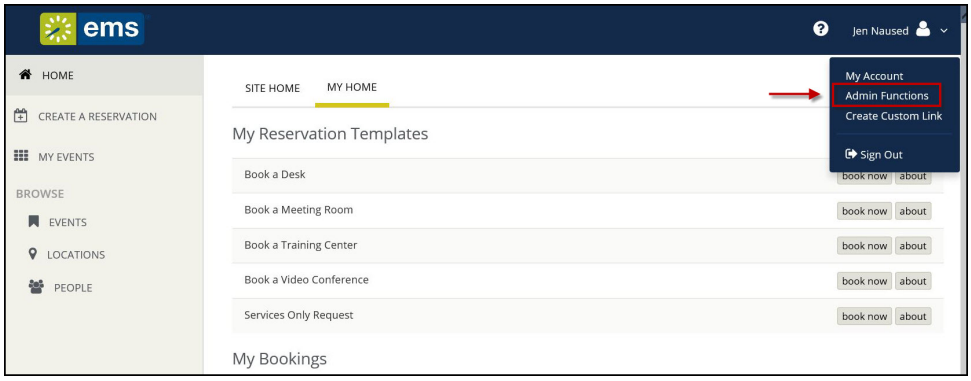
Configure Your LDAP Provider

1. Navigate to Platform Services admin portal (e.g., https://Yourcompany.com/EmsPlatform/admin) and select Integrations from the sidebar.

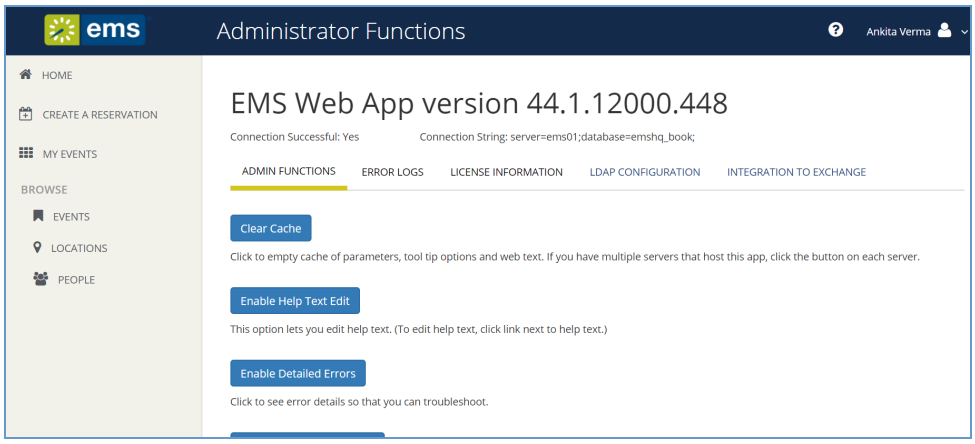
2. Select EMS Mobile and choose LDAP from everyday user authentication method dropdown.



3. Navigate to the **EMS Web App** > **Admin Functions** page, listed under your name in the upper right corner of the application.



4. Tap the **LDAP Configuration** tab and complete all required LDAP information, and then test your configuration.

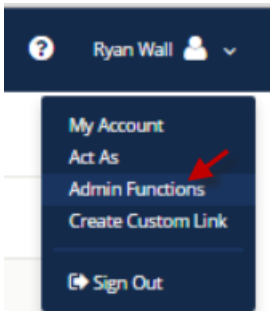


Note:

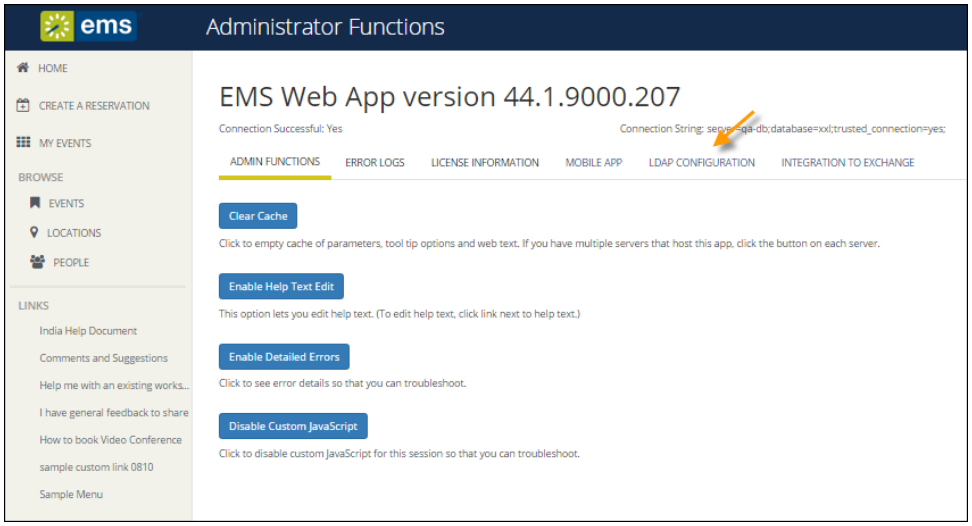
This is the same process you use for authenticating EMS Web App with LDAP. The EMS Platform Services API uses the same configuration information.

Configure EMS Web App to Use LDAP Authentication

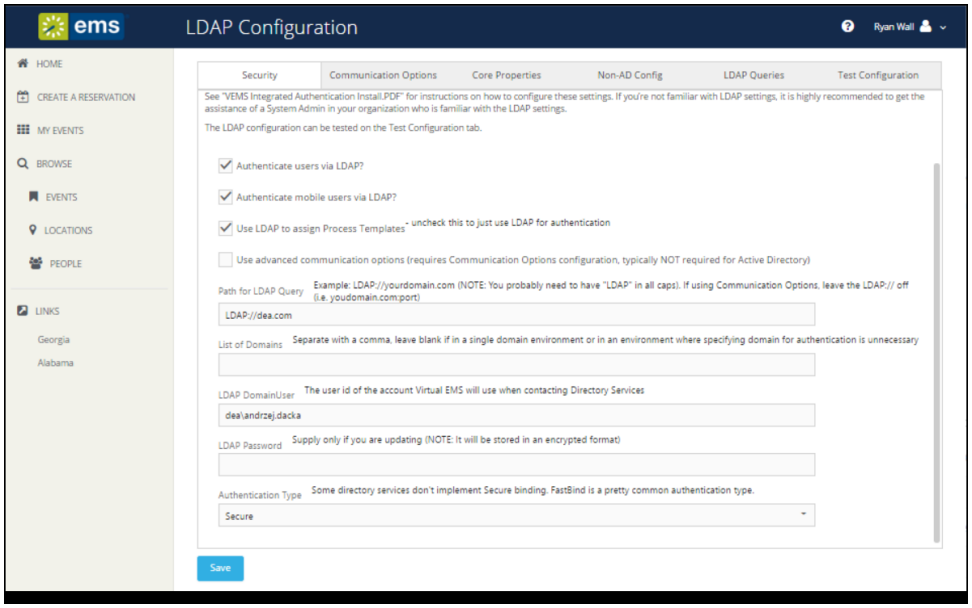
1. Log into EMS Web App with a User that belongs to an Everyday User Security Template containing the Web Administrator role (controlled in the EMS Desktop Client under Configuration > Everyday User Applications > Everyday User Security Templates). See Also: Configuring Security Templates
2. From the User Options, select Admin Functions.



3. Click the LDAP Configuration tab.



4. The LDAP Configuration window appears, presenting multiple tabs for various settings.



Configure EMS Web App Security

To configure EMS Web App security, complete the following from the **Security** tab:

1. Select the Authenticate users via LDAP checkbox to enable LDAP authentication.
2. If LDAP will be used to assign Everyday User Process Templates to your Web Users, select the Use LDAP to assign Process Templates checkbox.

3. Use advanced communication options: Skip this step for Active Directory environments. Enabling this checkbox requires that you complete the settings on the Communication Options tab.
4. In the Path for LDAP Query field, specify a valid LDAP path (example – LDAP://YourCompany.com)
5. List of Domains: Skip this step if your organization uses a single domain. Otherwise, provide a comma separated list of your domains.
6. In the LDAP Domain\User field, enter a Domain User account that has rights to query LDAP (example – YourDomain\User)
7. In the Password field, enter a valid Password for the User Account entered in the previous step.
8. Specify the appropriate LDAP Authentication Type for your environment.

Note:

The other tabs (Communication Options, Core Properties, Non-AD Config and LDAP Queries) should only be edited with assistance from our Support Department when special circumstances arise with unique configurations of LDAP.

Configure Communication Options

Important!

It is recommended that this tab only be edited with assistance from our Support Department when special circumstances arise with unique configurations of LDAP. If you're not familiar with the LDAP settings, it is highly recommended to get the assistance of a System Admin in your organization who is familiar with the LDAP settings.

The Communication Options tab includes fields that define how to fetch a Group or a User when sending communications from the EMS Desktop Client. You can also set the SSL configurations, including the Security Certificate Path. Checking the Use SSL box will force communication to use SSL.

- **Certificate Path**: If there is a specific certification that you want to use to validate your authentication.
- **Authentication Type**: Type of authentication that your LDAP server will use during the binding process. Basic is the default because it is the most common.
- **Search Root**: The root is the level at which your search will begin.
- **User Search Filter**: Specifies the filter to use when performing the user search.
  - Example: (&(objectClass=Person)(SAMAccountName={0})) or (&(objectClass=Person)(uid={0}))
- **Group Search Filter**: Specifies the filter to use when performing the group search.
  - Example: (&(objectClass=Person)(objectClass=user))

- **Protocol Version**: Insert the current version number here. The default is 3, as the current version should be 3.

Core Properties

> **Important!**
> It is recommended that this tab only be edited with assistance from our Support Department when special circumstances arise with unique configurations of LDAP. If you're not familiar with the LDAP settings, it is highly recommended to get the assistance of a System Admin in your organization who is familiar with the LDAP settings.

Indicate whether your LDAP implementation is Active Directory. These properties are set to the common defaults, but can be changed here if the LDAP properties differ from the defaults displayed.

- **LDAP Name Property**: The property for user name on the user record in LDAP that will be displayed. Displayname is the default, as it is the most common.
- **LDAP Phone Property**: The property for the phone number on the user record in LDAP that will be displayed. Telephonenumber is the default, as it is the most common.
- **Domain to append to users**: This field is unnecessary unless the domain of your user is different from the domain returned from the query.
- **Field for LDAP Group Lookup**: This identifies the EMS property that should be utilized when performing the search. For example, if you use LDAP solely to assign templates and you want the EMS Web App to look up group membership using a field other than the login name, then you must enter that field's name here.

Non-AD Configuration

> **Important!**
> It is recommended that this tab only be edited with assistance from our Support Department when special circumstances arise with unique configurations of LDAP. If you're not familiar with the LDAP settings, it is highly recommended to get the assistance of a System Admin in your organization who is familiar with the LDAP settings.

If your LDAP implementation is not Active Directory, use these fields to redefine the LDAP property names used when searching directory information.

- **LDAP Account/User ID Property**: The property in your LDAP store that contains the user name.
  - Example: If sameaccountname=xxxx, then enter sameaccountname

- **Full LDAP User ID Format**: Leave blank unless authentication requires a full path.
  - Example: cn={0},ou=staff,o=yourdomain
- **LDAP Group Category**: The property in your LDAP store that contains the group category.
  - Example: If filter should be objectClass=groupOfNames, then property should be groupOfNames
- **LDAP Group Name**: The property in your LDAP store that contains the group name.
- **LDAP Group Member Name**: The property in your LDAP store that contains the name of a single member in the group.
  - Example: If member property is member=jdoe, then property should be member
- **LDAP Group Member User Name Attribute**: The property of the user record that corresponds to the group's member property to determine group membership.

LDAP Queries

Important!

It is recommended that this tab only be edited with assistance from our Support Department when special circumstances arise with unique configurations of LDAP. If you're not familiar with the LDAP settings, it is highly recommended to get the assistance of a System Admin in your organization who is familiar with the LDAP settings.

These are LDAP query overrides to fetch Groups and Users from the domain. These settings rarely need to overridden, but can be used to customize queries.

- **LDAP query for security groups**: Query used to search for security groups in your LDAP store.
- **LDAP query to find users**: Query used to search for users in your LDAP store.
- **LDAP query for find users with space**: Query used to search for users that have spaces surrounding their user names in your LDAP store.

Save Your Configuration

1. Click Save.

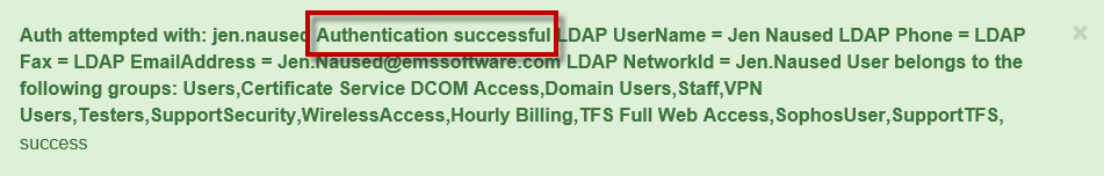
Note:

If you want Everyday Users to inherit Everyday User Process Templates based on the LDAP Group(s) with which they belong, see LDAP Groups Tab. Otherwise, you have completed the configuration process.

2. Within EMS Desktop Client, go to the Everyday User Process Templates area (Configuration > Web > Everyday User Process Templates).
3. Within an Everyday User Process Template, locate the LDAP Groups tab and select the appropriate LDAP Group(s) to map to that Everyday User Process Template.
4. Click OK.

Test Your Configuration

1. After completing configuration, navigate to the **Test Configuration** tab in the EMS Web App under LDAP Configuration.
2. Enter your Network UserId Without Domain Name.
3. Enter your Password.
4. Click **Test**.
   a. If your configuration was successful, you will receive a message in a green box at the top that includes domain information and the words "Authentication successful" (please see example below).



   b. If the configuration was unsuccessful, you will receive a prompt stating that LDAP could not be accessed. Check your logs to determine the reason for the failure.

Configuring Authentication for the EMS Mobile App

1. If your organization uses EMS Mobile App, click the **Mobile App** tab.
2. Choose the LDAP option.

Test Your LDAP Configuration

Assuming you have installed the EMS Platform Services at https://Yourcompany.com/EmsPlatform, then you can test the configuration with a simple curl command:

```
curl -X GET -H 'x-ems-consumer: MobileApp' https://em-
s.yourcompany.com/endpoint/api/v1/health
```

> **Note:**
> You can also use the API's Swagger interface to accomplish this goal.

You should see a portion of the JSON response that looks like this (unrelated details omitted for brevity):

```
{
    ...
    "additionalProperties": {
        "authConfig": {
            "activities":"ldap"  // <-- these are the crit-
ical lines
            "ui":"ldap"
        }
    }
}
```

Test Your LDAP Authentication

Assuming you have installed the EMS Platform Services API at https://ems.*yourcompany*.com/endpoint, you can test the authentication with a simple curl command:

```
curl -X POST -H 'x-ems-consumer: MobileApp' -H 'Content-
Type: application/json' -d '{"username":

"your_username", "password":"your_password"}' https://em-
s.yourcompany.com/endpoint...authentication
```

...where your_*username* and your_*password* are your credentials.

> **Note:**
> **api/v1/authentication** is the endpoint within the API where your request must be sent.

CHAPTER 14: Open ID Connect Authentication

This section guides you authenticating your users via the Open ID Connect protocol. Authentication with Open ID requires configuration in EMS Mobile App before users can authenticate.

> **Note:**
> For more information about how Open ID can be hosted or pre-configured in the EMS Mobile App, see Open ID Connect Authentication Can Be Hosted or Pre-Configured in the EMS Mobile App.

This topic provides information on the following:

OpenID authentication configuration requires two inputs:

1. User Info Endpoint. The EMS Platform Services will send the access_token to this endpoint to retrieve information about the end user.
2. Specify whether the EMS Platform Services should make a GET or POST request to the userinfo end-point.

Register Your EMS Mobile App with idP

This is your responsibility. The client_id generated by this registration is required.

Customize Your Configuration

Follow the steps below to customize your Open ID Connect configuration.

Create a Configuration File

1. Refer to Customize Your Mobile App Configuration Using config.json for details on building a configuration file for EMS Mobile App.
2. Once you have created your configuration file, you might proceed with one of the sections below, depending on whether you intend to host the file or pre-configure the application and redistribute it.

Use Hosted Configuration

Host your configuration file from a web server an distribute the URL to your end users via the Import SSO Config feature in EMS Mobile App. Users should only have to perform this import one time per installation of the application.

Important!

It is not recommended to make this configuration file available publicly, since it will likely have URLs and/or other information in it that you do not want made available. Instead, host the file such that it is only available internally to your organization.

Pre-Configure EMS Mobile App

If you want to pre-configure the mobile app, see Configure and Re-Sign the EMS Mobile App.

Test Your Open ID Connect Configuration

Assuming you have installed the EMS Platform Services API at https://ems.yourcompany.com/endpoint, then you can test the configuration with a simple curl command:

```
curl -X GET -H 'x-ems-consumer: MobileApp' https://em-
s.yourcompany.com/endpoint/api/v1/health
```

Note:

You can also use the API's Swagger interface to accomplish this goal.

You should see a portion of the JSON response that looks like this (unrelated details omitted for brevity):

```
{
    ...
    "additionalProperties": {
        "authConfig": {
            "activities": "openId"  // <-- these are the
critical lines
            "ui":"openId"
        }
    }
}
```

Test Your Open ID Connect Authentication

Assuming you have installed the EMS Platform Services API at https://ems.*yourcompany*.com/endpoint, you can test the authentication with a curl command:

```
curl -X POST -H 'x-ems-consumer: MobileApp' -H 'Content-
Type: application/json' -d '{"token":

"your_access_token"}' https://em-
s.yourcompany.com/endpoint...authentication
```

...where your_*access_token* is a valid *access_token* retrieved from your IdP.

Note:

api/v1/authentication is the endpoint within the API where your request must be sent.

CHAPTER 15: Open ID Connect Authentication Can Be Hosted or Pre-Configured in the EMS Mobile App

Hosted Configuration: The configuration can be hosted at a URL available to end users. The user will then enter that URL into the application. EMS Mobile App will download and use that information, and kick off the authentication process. When configured this way, users will launch the EMS Mobile App and see the EMS Server URL screen. Instead of entering an EMS Server URL, the user will tap **About** near the bottom right of the screen and select the option to **Import SSO Configuration**. The user will then tap **Import** Mobile app, which will direct the user to enter the Configuration URL. Then the user will tap **Import**.

Pre-Configured In EMS Mobile App: The configuration can be "baked" into the application. This requires re-signing, hosting, and re-distributing the EMS Mobile App within your organization. With a pre-configured EMS Mobile App, users do not need to import any Open ID configuration details. EMS Mobile App will launch with that configuration and use it directly.

How Users Authenticate After Configuration

Assuming successful import of the configuration data, the authentication flow can now begin. EMS Web App will show the user the Open ID authorization web page (this happens in a web view inside the EMS Mobile App, and the user might briefly see a busy indicator while the page loads). The user will authenticate with the Open ID authorization view. The user plays no part in these next steps, which describe the completion of the Open ID flow. The user might simply see the screen change during this process. Successful authentication will redirect the user back to EMS Web App. EMS Web App will resume the Open ID authentication process and retrieve and access_token from the identity provider and will then forward the access_token to the EMS Platform Services API. EMS Platform Services API will verify the access_token by making a userinfo request per the Open ID specification. EMS Platform Services API will authenticate the user by matching the login email field (if provided) to an Everyday User in the EMS database. If there is no email field in the response, the API will try to match the response's sub field to an Everyday User. EMS Platform Services API will respond to EMS Mobile App. Once Open ID workflow above has successfully completed, EMS Web App will direct the user to the Home screen. If the EMS Platform Services API is unable to verify the credentials, EMS Mobile App will inform the user based on that response.

How the Identity Provider (IdP) Works

The Identity Provider (IdP) handles the input and verification of end user credentials. It also issues and verifies tokens. The EMS Mobile App must be registered with the IdP. The client_id generated by this registration is required information for the configuration used by the EMS Mobile App and the Open ID flow.

How the EMS Platform Services API Works

The EMS Platform Services API receives the access_token from the EMS Mobile App. The token is then sent to the userinfo endpoint for verification. The response from the userinfo endpoint is used to find a user in the EMS database. The API will then respond to the EMS Mobile App based on the results of this process.

CHAPTER 16: Persistent and 2-Factor Authentication

Persistent Authentication refers to the ability of the EMS Mobile App to automatically log users in so that they are not required to log into EMS Mobile App every time they need to access it. When using persistent authentication, a user's EMS Mobile App credentials will become invalid after a period of inactivity equal to or greater than the duration defined in settings. If not using persistent authentication, a user will be forced to re-authenticate after the duration defined in settings has elapsed, regardless of activity.

Two-factor (2fa) refers to the ability of the EMS Mobile App to confirm a user's identity by granting access only after successfully presenting two or more pieces of evidence to an authentication mechanism. This gives EMS Administrators an enhanced security option for their EMS Everyday Users.

Important!

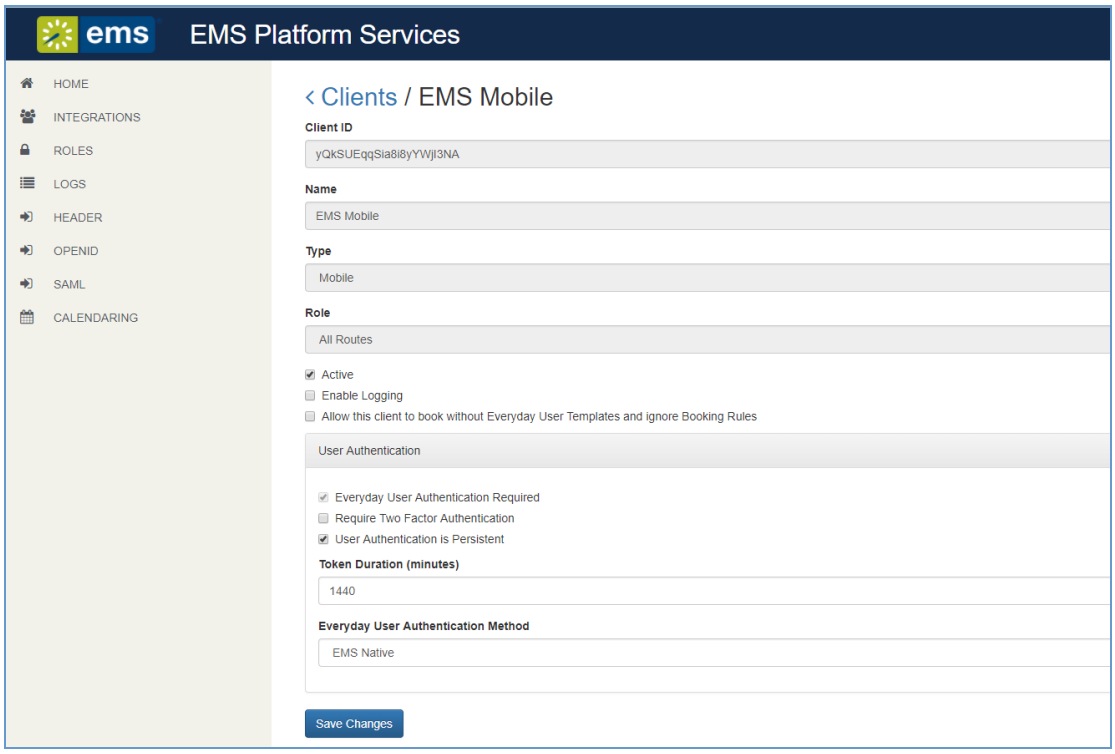
Both Persistent and 2fa are available through Native, Windows, and LDAP authentications.

Persistent Authentication

Note:

Users with persistent authentication will be prompted to log back in to EMS Mobile App if anything is changed about their profile in EMS Desktop Client on the Everyday Users tab, such as Email, Password, External Reference, Network ID, and Security Template. If you remove a user's access to a process template, they will also be alerted when they attempt to use it, and then they will be prompted to re-authenticate.

1. Navigate to the EMS Platform Services Admin Page.
2. Click the Integrations tab.
3. Click on EMS Mobile.
4. Select the **User Authentication Is Persistent** checkbox.
5. Set the token duration in minutes.



6. Click **Save**.

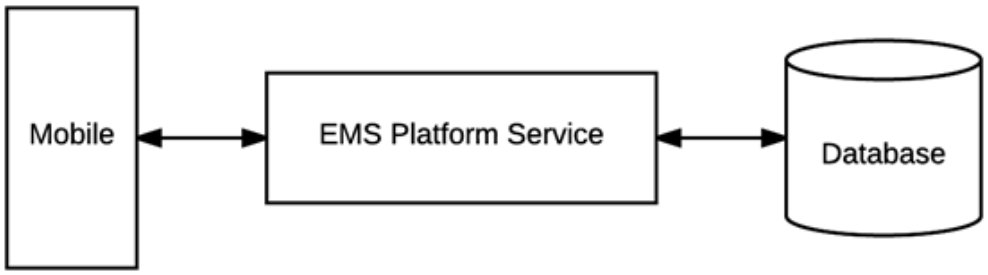
> **Note:**
> This setting overrides the token duration sent by SSO providers. If a user should leave your organization, you should manually disable his or her profile in EMS, otherwise the employee will have access to EMS Mobile App for the duration defined above. You can also use to streamline this process.

Two-Factor (2fa) Authentication

1. Enable the 2fa parameter in EMS Desktop Client.
2. Navigate to the EMS Platform Services Admin Page.
3. Click the Integrations tab.
4. Click on EMS Mobile.
5. Select the **Require Two Factor Authentication** checkbox.

CHAPTER 17: EMS Native Authentication

Authenticate your users via Everyday Application User (emsuser) credentials stored in the EMS database. The following example shows the default configuration that ships with EMS Mobile App.



Example EMS Native Authentication in the EMS Mobile App

After successful connection to EMS Platform Services, the user will:

1. Enter his or her credentials on the Sign In screen.
2. Tap **Sign In**.
3. User will be taken to the Home screen.

If the credentials are missing or invalid when the user taps **Sign In**, an error message will appear indicating invalid credentials or that the fields are required.

Test Your EMS Native Authentication

Assuming you have installed the EMS Platform Services at https://Yourcompany.com/EmsPlatform, then you can test the authentication with a curl command:

```
curl -X POST -H 'x-ems-consumer: MobileApp' -H 'Content-Type: application/json' -d '{"username":

"your_username", "password":"your_password"}' https://ems.yourcompany.com/endpoint...authentication
```

...where your_*username* and your_*password* are your credentials.

> **Note:**
> **api/v1/authentication** is the endpoint within the API where your request must be sent.

CHAPTER 18: Add Mobile Users

EMS Mobile App users are added as "Everyday Users" in EMS Desktop Client. Follow the steps below to create this type of user.

This section guides you in configuring one Everyday User at a time. Once you have configured these users, you might need to assign them to security templates and one or more process templates.

- To assign users to Everyday User process templates, see also: Assign Templates to Everyday Users.
- To assign multiple templates to multiple users in a single step, see also: Assign Security Templates to Multiple Everyday Users.

Note:

You configure EMS Desktop Client user accounts in a different area (under the **System Administration** > **Security** menu). For instructions, see Configure EMS Desktop Client Users.

Additionally, if your organization uses EMS Human Resources Toolkit to manage Everyday User accounts, see also: EMS Human Resources Toolkit.

Lastly, a set of Account Management parameters control account management behavior. To view these parameters, see also: EMS Web App Parameters.

Concept: EMS classifies users into two categories—Guests or Visitors and Everyday Users.

"Guests" or "Visitors" (unauthenticated or anonymous users) can browse events, see details about your organization's space, and/or submit requests.

These users can register themselves through the EMS Web App and create a user account. To enable this, you need to set certain account management parameters (see also: EMS Web App System Parameters) and select the Credit\Edit an Account role for the unauthenticated user (see the Roles tab definition in Configuring a Security Template).

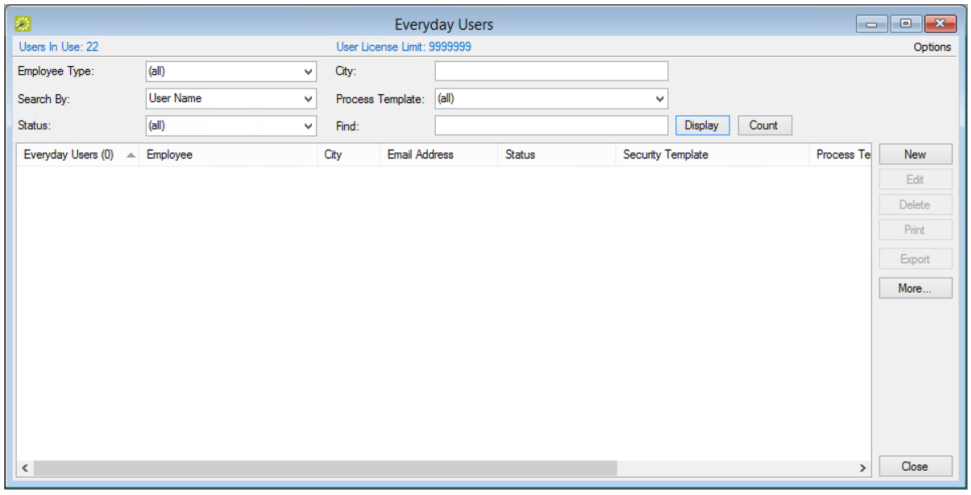
"Guests" or "Visitors" (authenticated users) might also submit and manage reservations if you enable them. You can configure these users through the EMS Desktop Client or the optional Integrated Authentication module.

See Also: Configure Additional Information for a Group and Configure Contacts. Before you configure a user, check that the user has not already been created.

Everyday User process templates control access and behavior in EMS Software's Everyday User Applications. If you are upgrading from an older release of EMS, you might recognize Everyday Users as "Web Users" and "Everyday User Process Templates" as "Web Process Templates."

1. On the EMS Desktop Client menu bar, click **Configuration** > **Everyday User Applications** > **Everyday Users**. The Everyday Users window opens. The number of configured users for EMS Web App shows

in the upper left corner. The number of users for which your organization is licensed shows in the top center.



2. Check that the user you want to configure does not already exist.
   a. Enter the user name or email address in the **Find** field.

> **Note:**
> This search string is not case-sensitive, but your entries must be in the correct order. For example, if searching by Email Address, a search string of bob returns bobworth@emssoftware.com but not dbobbett@emssoftware.com.

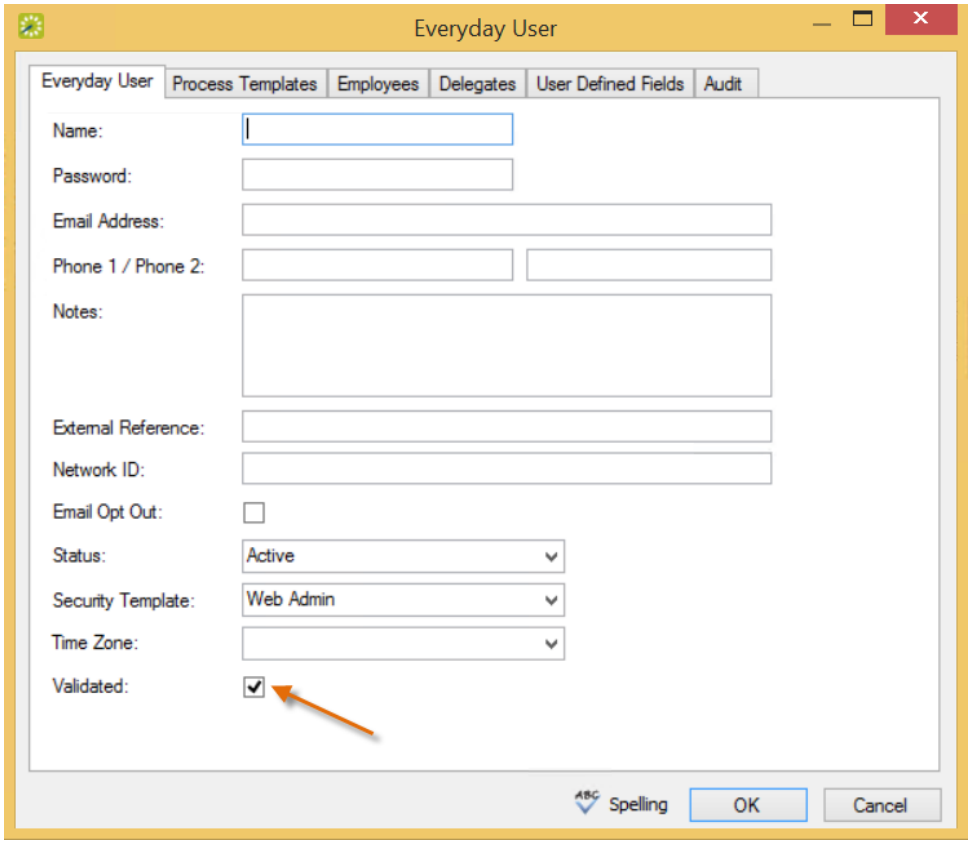
   b. Narrow your search results by:
      - Group Type
      - City
      - Status
      - Process Template

   c. Click **Display**. Search results show in the lower pane of the window. If your user does not already exist in EMS, proceed to the next step.

> **Note:**
> If the EMS system parameter **Users linked to Groups via External Reference** is set to **Yes**, then you will also see a Group column and a City column.

3. Create a new user. Click the **New** button. A dialog box opens.

> **Note:**
> If the user has confirmed membership (by responding to an email containing an activation link), the **Validated** checkbox highlighted below will be selected. If the user had to answer questions when requesting an account, you can view the user's responses on the **User Defined Fields** tab.



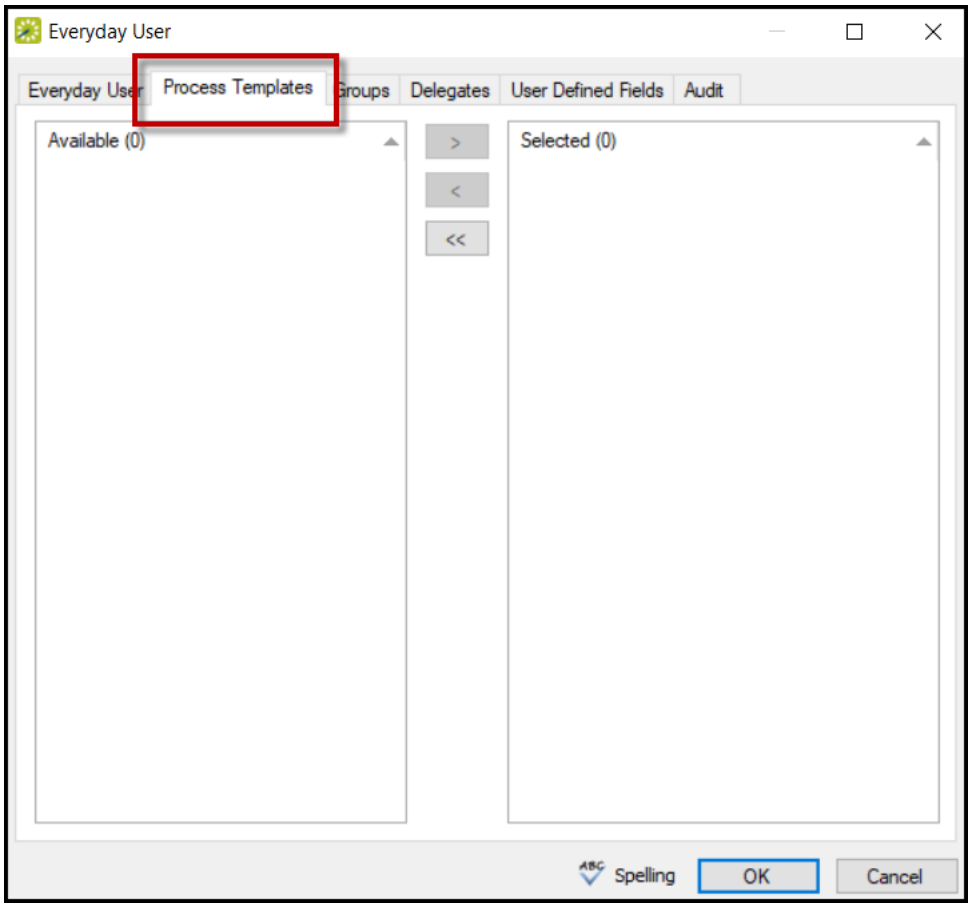
> **Note:**
> When you configure a user, you can also specify one or more delegates for the user from the Delegates tab. A delegate is a user who can create and view reservations on behalf of another user.

4. Enter information for the new user. User name and email address are required; password is only required if not using the optional Integrated Authentication module. All other information is optional and can be added later as needed.

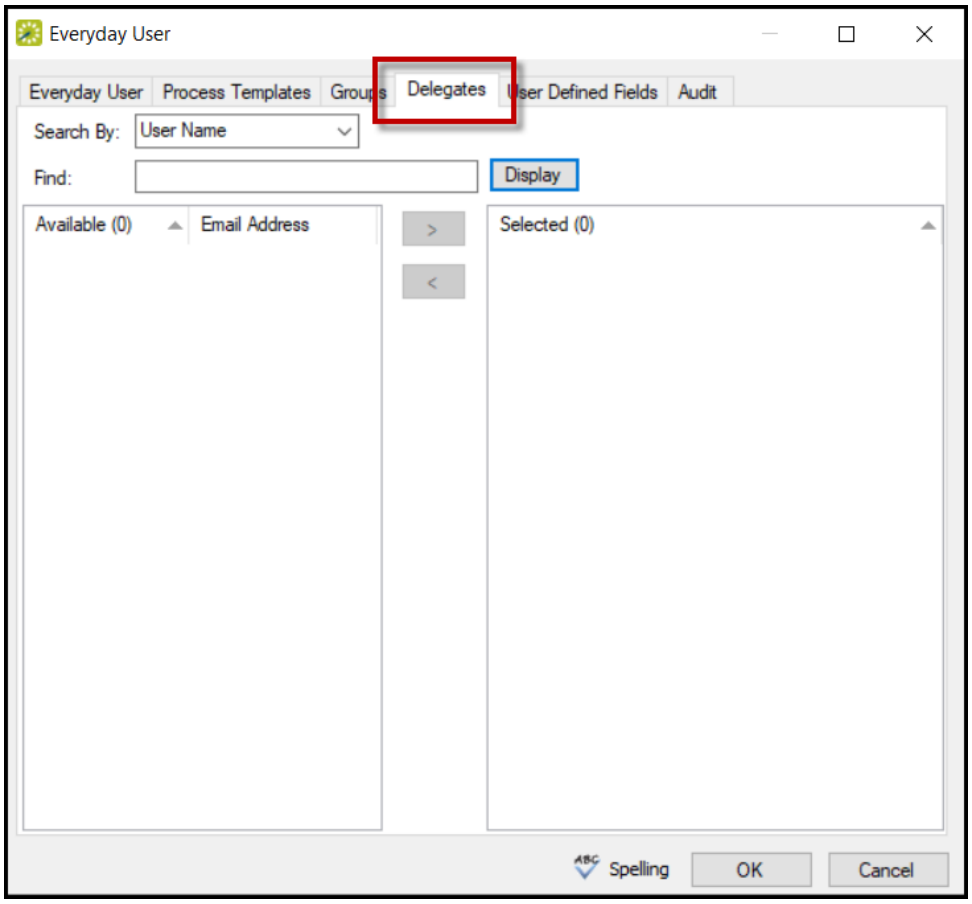
Field	Description
Name	REQUIRED. The name of the user. (Maximum of 30 characters, including spaces.)
Password	The password that the user must enter to log in to the EMS Web App. If using the optional Integrated Authentication module, Password can be left blank since the network password is used instead.
Email Address	REQUIRED. Enter the full email address for the user. Users must enter this email address to log in to the EMS Web App.
Phone 1 /Phone 2	OPTIONAL
Notes	OPTIONAL. Read-only.
External Reference	OPTIONAL. Links the user to an outside program, such as EMS Human Resources Toolkit, if needed.
Network ID	The user's network ID.
Email Opt Out	OPTIONAL. Select this option if you do not want the user to receive automatic emails (such as reservation summary emails) from the EMS Web App. The user can still receive manually sent emails.
Status	REQUIRED. Select the status for the user: • **Active**—The user can log in to EMS Web App, EMS Mobile App, and EMS for Outlook. • **Pending**—The user cannot log in to EMS Web App, EMS Mobile App, and EMS for Outlook and is informed that he/she must check back at a later time. • **Inactive**—The user cannot log in to EMS Web App, EMS Mobile App, and EMS for Outlook and is instructed to contact the EMS administrator.
Security Template	REQUIRED. This determines the user's access to the system (i.e., the menu items the user can see and the event information that the user can view).
Time Zone	OPTIONAL. The time zone in which the user is located.

Field	Description
	Note: As of Version 44.1, EMS Software strongly recommends that time zones are assigned to users for an optimal experience on all Everyday User Applications.
Validated	When checked, users who created their own accounts have confirmed membership (by responding to an email containing an activation link). When unchecked, the user will not be able to use the EMS Web App.

5. Open the **Process Templates** tab to assign process templates to the new user. Select one or more Process Templates listed in the Available column (use CTRL-click for multiple groups), and then click **Move** (**>**) to move the selected groups to the **Selected** list. The process templates you assign here will appear as menu items to the user in the EMS Web App, EMS Mobile App, and EMS for Outlook.



6. From the **Groups** tab, specify Groups on whose behalf the user can create and manage reservations. To filter the list of active groups displayed, use the **Find** and **Type** fields and then click **Display**. Select one or more Groups (use CTRL-click for multiple groups), and then click **Move** (**>**) to move the selected groups to the **Selected** list.
7. Specify Delegates the user can impersonate from the **Delegates** tab. To see all available users, click **Display**. To narrow the search results, use the **Search** by dropdown list to search by User Name or Email Address. Select one or more delegates (using CTRL-click for multiple delegates), and then click **Move** (**>**) to move the selected users to the **Selected** list.



Note:
Click the **Spelling** icon to spell-check any information that you manually entered for the user.

8. Click **OK**. The dialog box closes and returns you to the users window with the newly configured user automatically selected.

CHAPTER 19: Deploy EMS Mobile App

There are two ways to deploy the EMS Mobile App for your users:

1. Public Deployment—The standard public app store offered by Apple and Google.
2. Private Deployment—A private enterprise app store. (This approach can also be integrated with your company's Mobile Device Management system.)

Important!

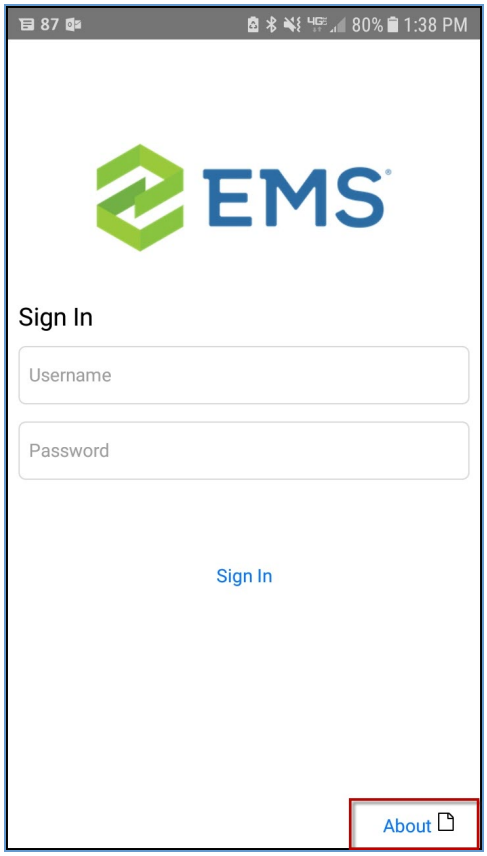
It is important to understand the compatibility between the EMS Mobile App and EMS Platform Services. The EMS Mobile App needs to be on the same version or higher as EMS Platform Services. For example, the EMS Mobile App Update 20 version will be compatible with EMS Platform Services Update 19 or older. However, compatibility issues will exist if you try to install EMS Platform Services Update 20 with an older version of the EMS Mobile App (Update 19 or older).

Public Deployment: Public App Store

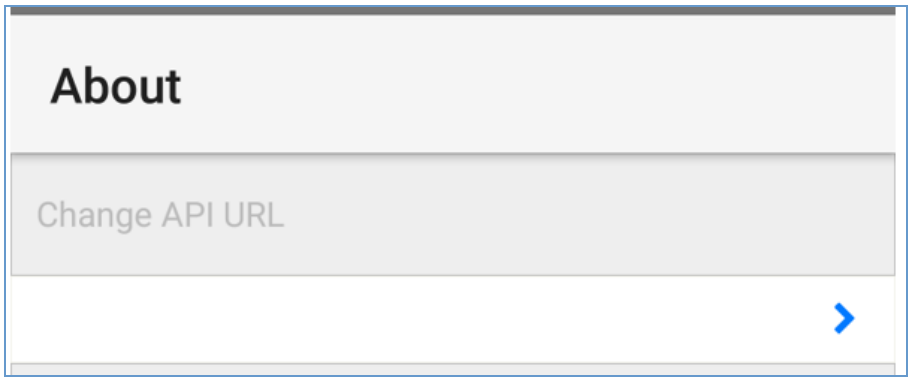
To deploy via the public app store, direct users to the Google Play and Apple app stores on their mobile devices. They will be able to download the EMS Mobile App by clicking on the link. However, they will have to manually input the EMS Mobile API URL. They will receive a prompt to do so the first time they open the EMS Mobile App.

If users need to change the API URL at a later date, they can:

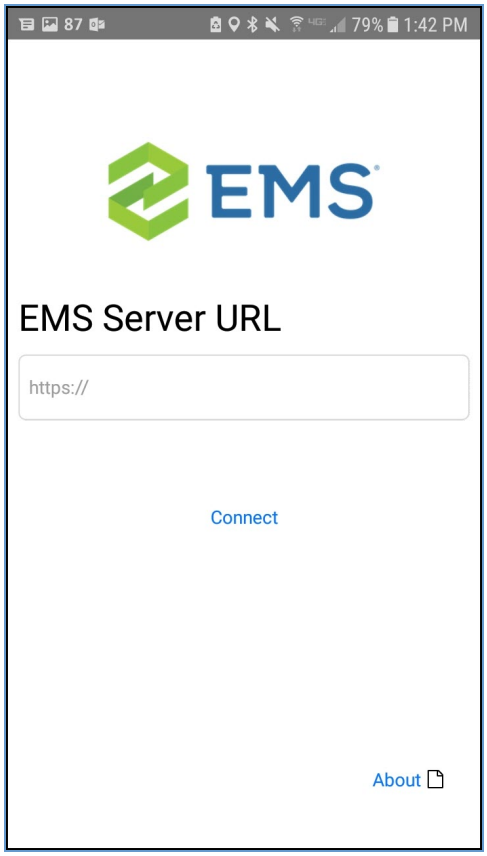
1. Open the EMS Mobile App, and then click **About** in the lower right corner.



2. Click to change the API URL.



3. Enter the API URL you provide and connect.



Important!

While Public Deployment might be easier for your IT staff, please consider the following:

- Users will have to input the EMS Mobile App API URL on their own.
- EMS will frequently deploy EMS Mobile App updates to the app store. Most users will have this app set to automatically update and will receive updates even if you have not yet upgraded your EMS Mobile API.
- While EMS Software aims to make the Mobile API backwards- and forwards-compatible within major updates, we might not do so all the time.
- Deploying via the public app store requires you to make major updates to the EMS Mobile API as soon as they are available.

Private Deployment: Private App Store

To deploy via a private enterprise app store, first download the unsigned apk/ipa files from the Downloads area of Accruent Access. You then have to resign the app and deploy it via your MDM system. This site offers some guidance on how to sign an unsigned ipa file (i.e. for iOS), while this site does the same for

Android apk files. Deploying via a private app store allows you to control which version of the EMS Mobile App your users have.

As an example, here are the key steps to resign and deploy the unsigned EMS Mobile App ipa file (following instructions provided here):

1. Download unsigned builds: .ipa and .apk files
    - Optional: Customize Your Mobile App Configuration Using config.json (Private Deployment Only)
2. Configure and Re-Sign the EMS Mobile App (Private Deployment Only)
    - Change the EMS Mobile App Logo (Private Deployment Only) (if using MDM)

CHAPTER 20: Change EMS Mobile App Logo (Private Deployment Only)

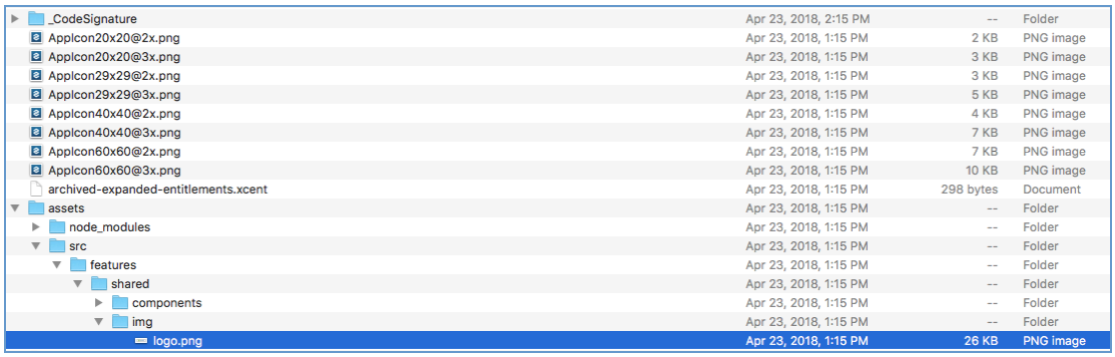
For customers re-signing the application, we provide unsigned builds.

This topic provides information on:

- Change the EMS Mobile App Logo in iOS
- Change the EMS Mobile App Logo in Android

Change EMS Mobile App Logo (iOS)

1. Store your unsigned EMS Mobile App in a new or empty directory.
2. Change the extension of the app to .zip. (e.g., IPhone.App-44.1.xxx-unsigned.ipa -> IPhone.App-44.1.xxx-unsigned.zip.)
3. Un-compress/expand the new zip file.
4. To set a custom logo, navigate to **Assets > SRC > Features > Shared > IMG.**



5. Replace the **logo.png** file.
6. Rezip all of the extracted files above.
7. Give the new zip file an ipa extension.
8. Using a Mac computer, install fastlane.
    - sudo gem install fastlane
9. Do the rest of this on your local directory.

10. Login to https://developer.apple.com and switch to team "Your Team Name."
11. Download your teams Distribution provisioning profile.
12. Double click it to install it. This file should exist on your system:
    - ~/Library/MobileDevice/Provisioning Profiles/<a guide for your provisioning profile>.mobileprovision
13. Get your team's existing .p12 file with the cert and private key combined, and then import that into Keychain (by double-clicking it) and then entering the password.
    - When the cert is installed successfully you should see iPhone Distribution: <Your Team Name> in your Keychain, with a private key.
14. Assuming you have:
    - fastlane installed on your Mac.
    - the cert & private key installed in Keychain
    - the provisioning profile mentioned above in: ~/Library....mobileprovision
15. Resign your target ipa with this command:

```
fastlane run resign \
ipa:path/to/your/file.ipa \
signing_identity:"iPhone Distribution: <Your Team Name>" \
provisioning_profile:$HOME/Library/MobileDevice/
Provisioning Profiles/<your profile GUID>.mobileprovision \
display_name:EMS-Resigned
```

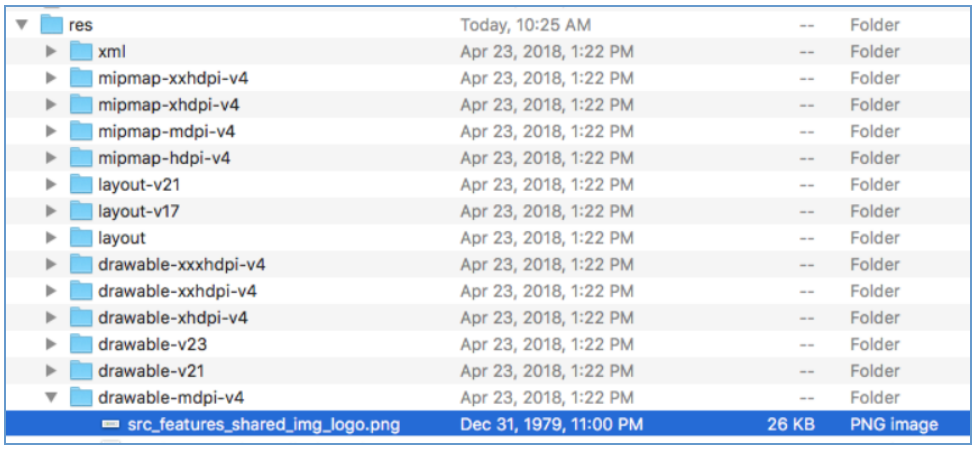
Note:

If you want a bash script that will do this, copy this into a file (e.g., resign_enterprise.sh):

```
#!/bin/bash
IPA=relative/path/to/file.ipa
IDENTITY="iPhone Distribution: <Your Team Name>"
PROFILE=$HOME/Library/MobileDevice/Provisioning Profiles/
<your profile GUID>.mobileprovision
DISPLAY_NAME=EMS-Resigned
fastlane run resign ipa:"$IPA" signing_identity:
"$IDENTITY" provisioning_profile:"$PROFILE" display_name:
$DISPLAY_NAME
```

Change EMS Mobile App Logo (Android)

1. Store your unsigned EMS Mobile App in a new or empty directory.
2. Change the extension of the app to .zip. (e.g., IPhone.App-44.1.xxx-unsigned.ipa -> IPhone.App-44.1.xxx-unsigned.zip.)
3. Un-compress/expand the new zip file.
4. To set a custom logo, navigate to RES > **Drawable-mdpi-v4**.



5. Replace the **src_features_shared_img_logo.png** file.
6. Rezip all the extracted files above.

> **Important!**
> Assets, Res, and AndroidManifest.xml are top-level files in an .apk. Please ensure you are zipping the correct files.

This CLI command will zip all the files in the current directory into a new zip file in the parent directory:

```
zip -qr ../ems-custom-44.1.xxx.zip ./*
```

7. Give the new zip file an apk extension (e.g., myapp.zip -> myapp.apk).
8. Sign the new apk file.
9. The script below is what EMS uses to sign the EMS Mobile App. Please adjust for your needs:

```
#!/bin/bash

APK_TO_SIGN=$1

APK_OUTPUT=$2

EMS_APK_KEYSTORE_PATH=path/to/your/app.keystore


jarsigner -verbose \

-sigalg $EMS_APK_SIG_ALG \

-digestalg $EMS_APK_DIGEST_ALG \

-storepass $EMS_APK_KEYSTORE_PASS \

-keystore $EMS_APK_KEYSTORE_PATH \

$APK_TO_SIGN $EMS_APK_ALIAS_NAME


zipalign 4 $APK_TO_SIGN $APK_OUTPUT
```

Note:

EMS recommends that you use an image with a 3:1 aspect ratio in order to ensure that the image will be properly rendered by the application.

CHAPTER 21: Configure and Re-Sign the EMS Mobile App (Private Deployment Only)

This topic provides information on the following:

Use Unsigned Builds

For customers re-signing the application, we provide unsigned builds.

1. Store your unsigned EMS Mobile App in a new or empty directory.
2. Change the extension of the app to .zip. (e.g., IPhone.App-44.1.xxx-unsigned.ipa -> IPhone.App-44.1.xxx-unsigned.zip.)
3. Un-compress/expand the new zip file.

Set Custom Configuration

1. Refer to Customize Your Mobile App Configuration Using config.json (Private Deployment Only) for details on building a configuration file for the EMS Mobile App.
2. Replace the config.json file with your custom configuration (located as follows):

IOS

config.json (top-level file)

Android

assets/config.json

Re-Sign and Repackage for iOS

Follow the steps below to re-sign and repackage for iOS.

1. Install Fastlane

Using sudo gem, install fastlane on an administrative Mac computer.

2. Install Certificate and Provisioning Profile

If your Mac computer is already configured with these items, these steps might not be necessary.

Provisioning Profile

1. Login to https://developer.apple.com.
2. Download your Distribution provisioning profile.
3. Double click it to install it. This file should exist on your system:
    - ~/Library/MobileDevice/Provisioning Profiles/<profile-guid>.mobileprovision

Certificate

See Apple's documentation for installing and managing certificates and signing identities. When the certificate is installed successfully, you should see iPhone Distribution: Your Company, Inc in your Keychain, with a private key.

3. Re-Sign

If you have the following, you should be ready to re-sign the EMS Mobile App:

- Fastlane installed on your Apple computer
- the cert and private key installed in Keychain
- the provisioning profile mentioned above in ~/Library/.../<profile-guid>.mobileprovision

Before proceeding, change the following in the command below:

- Replace path/to/your/file.ipa with the real path to the ipa file
- Replace iPhone Distribution: Your Company, Inc with the appropriate signing identity on your machine
- Replace <profile-guid> with the actual GUID or name of the provisioning profile you intend to use
- Replace **EMS-Resigned** with the display name you want to use, or remove the parameter if you do not want to rename the application

Note:
Running these commands will **overwrite** the ipa file you designate. Make a copy first if necessary.

```
fastlane run resign \
    ipa:path/to/your/file.ipa \
    signing_identity:"iPhone Distribution: Your Company,
Inc" \
    provisioning_pro-
file:$HOME/Library/MobileDevice/Provisioning Pro-
files/<profile-guid>.mobileprovision \
    display_name:EMS-Resigned
```

(All on one line for copy/paste:)

```
fastlane run resign ipa:path/to/your/file.ipa signing_iden-
tity:"iPhone Distribution: Your Company, Inc"
provisioning_profile:$HOME/Library/MobileDevice/Provisioning
Profiles/<profile-guid>.mobileprovision
display_name:EMS-Resigned
```

If you want a bash script that will do this, you can copy this into a file (e.g., resign_enterprise.sh):

```
#!/bin/bash

IPA=relative/path/to/file.ipa
IDENTITY="iPhone Distribution: Your Company, Inc"
PROFILE=$HOME/Library/MobileDevice/Provisioning\ Pro-
files/<profile-guid>.mobileprovision
DISPLAY_NAME=EMS-Resigned

fastlane run resign ipa:"$IPA" signing_identity:"$IDENTITY"
provisioning_profile:"$PROFILE" display_name:$DISPLAY_NAME
```

Re-Sign and Repackage for Android

- Re-zip all the extracted files from earlier
  - Note that assets, res, and AndroidManifest.xml are top-level files in an .apk, so be careful to zip the right files
  - This CLI command will zip all the files in the current directory into a new zip file in the parent dir-

ectory:

- zip -qr ../ems-custom-44.1.xxx.zip ./*

- Give the new zip file an .apk extension
  - e.g., myapp.zip -> myapp.apk
- Sign the new .apk file, for example:

```
#!/bin/bash

APK_TO_SIGN=$1
APK_OUTPUT=$2
EMS_APK_KEYSTORE_PATH=path/to/your/app.keystore

jarsigner -verbose \
    -sigalg $EMS_APK_SIG_ALG \
    -digestalg $EMS_APK_DIGEST_ALG \
    -storepass $EMS_APK_KEYSTORE_PASS \
    -keystore $EMS_APK_KEYSTORE_PATH \
    $APK_TO_SIGN $EMS_APK_ALIAS_NAME

zipalign 4 $APK_TO_SIGN $APK_OUTPUT
```

CHAPTER 22: Customize Your Mobile App Configuration Using config.json (Private Deployment Only)

EMS Mobile App ships with a config.json file that you can use to customize before re-signing and distributing in your app store or similar.

This topic provides information that will allow you to:

- Set the API URL so users do not have to type it in on their own.
- Configure authentication
- Find the config.json File
  - For iOS
  - For Android
- Supported Authentication Configurations
  - OpenID
  - SAML
- Change the Logging Location

Find the config.json File

After unzipping the respective app files, the paths to the file for each OS are:

iOS

- config.json (top-level file)

Android

- assets > config.json

The file looks like the example below (subject to change, per development):

```
{
    "api_doc": [
        "Configure the API here"
    ],
    "api": {

        "url_doc": [
            "The API EMS Mobile App should connect to"
        ],
        "url": ""
    }
}
```

Set the API URL

1. Open the **config.json** file in a text editor.
2. In the API section, find the URL property.
3. Set the URL property to your desired value (e.g., https://Yourcompany.com/EmsPlatform).

Configure Authentication

EMS Mobile App does not ship with an authentication configuration section by default, but you can add it as follows.

> **Note:**
> If you are adding authentication configuration, **it is also necessary to** set the API URL.

Below is an example (the ..._doc entries are omitted for brevity):

```
{
    "api": {
        "url": "https://yourcompany.com/EmsPlatform"
    },
    "authentication": {
        "activities": "openId",
        "openID": {
            "discoveryURL":
"https://yourcompany.com/openid",
            "authorizationURL": "",
            "tokenURL": "",
            "clientID": "abcdefxabQijQcJstY4nImWYL5y12345",
            "redirectURL": "emssoftware://oauth-callback/x"
        }
    }
}
```

Supported Authentication Configurations

Open ID

```
"authentication": {
    "activities": "openId",
    "openID": {
        "discoveryURL": "https://yourcompany.com/openid",
        "authorizationURL": "",
        "tokenURL": "",
        "clientID": "abcdefxabQijQcJstY4nImWYL5y12345",
        "redirectURL": "emssoftware://oauth-callback/x"
    }
}
```

- Set the **activities** to **openId**
- Add an **openID** section next to **activities**

Properties for the openID Section

- **discoveryURL**
  - if your IdP provides it, this is the URL for EMS Mobile App to automatically configure its Open ID settings.

- if you provide this, leave authorizationURL and tokenURL empty.

- **authorizationURL**
  - this is the endpoint to send the initial Open ID authorization request
- **tokenURL**
  - this is the endpoint to request an Open ID access token
- **clientID**
  - the client ID for the EMS Mobile App as configurd in the IdP
- **redirectURL**
  - leave this set to emssoftware://oauth-callback/x for EMS Mobile App
  - this is the URL the IdP will redirect to during the Open ID authentication flow

SAML

```
"authentication": {
    "activities": "saml",
    "saml": {
        "url": "https://yourcompany.com/ems-plat-
form...ntication/saml`
    }
}
```

- Set the **activities** to **saml**
- Add a **saml** section next to **activities**

Properties for the SAML Section

- URL
  - this property is optional
  - you can manually specifiy the initial request URL for SAML authentication
  - this URL will be opened in a webview in EMS Mobile App
  - if you do not specify this property, EMS Mobile App will assume the default SAML endpoint for the REST API
    - This is one reason you must specify the URL in the api section for custom authentication configuration (e.g., if you set the custom API URL to https://ems.example.com/api, then EMS Mobile App will use https://ems.example.com/api/api/v1/a...ntication/saml as its initial SAML url)

Examples

Custom URL only

```
{
    "api": {
        "url": "https://yourcompany.com/EmsPlatform"
    }
}
```

Open ID with Discovery URL

```
{
    "api": {
        "url": "https://yourcompany.com/EmsPlatform"
    },
    "authentication": {
        "activities": "openId",
        "openID": {
            "discoveryURL": "https://y-
ourcompany.com/openid/discovery",
            "authorizationURL": "",
            "tokenURL": "",
            "clientID": "abcdefxabQijQcJstY4nImWYL5y12345",
            "redirectURL": "emssoftware://oauth-callback/x"
        }
    }
}
```

Open ID without Discovery URL

```
{
    "api": {
        "url": "https://yourcompany.com/EmsPlatform"
    },
    "authentication": {
        "activities": "openId",
        "openID": {
            "discoveryURL": "",
            "authorizationURL": "https://y-
ourcompany.com/openid/authorize",
            "tokenURL": "https://yourcompany.com/openid/token",
            "clientID": "abcdefxabQijQcJstY4nImWYL5y12345",
            "redirectURL": "emssoftware://oauth-callback/x"
        }
    }
}
```

SAML with Default API SAML Endpoint

```
{
    "api": {
        "url": "https://yourcompany.com/EmsPlatform"
    },
    "authentication": {
        "activities": "saml"
    }
}
```

SAML with Specific API SAML Endpoint

```
{
    "api": {
        "url": "https://yourcompany.com/EmsPlatform"
    },
    "authentication": {
        "activities": "saml",
        "saml": {
            "url": "https://ems.example.com/saml"
        }
    }
}
```

Change Logging Location

1. Modify the logFilePath attribute:

```
"logFilePath": ".\\LogFiles\\api.log"
```

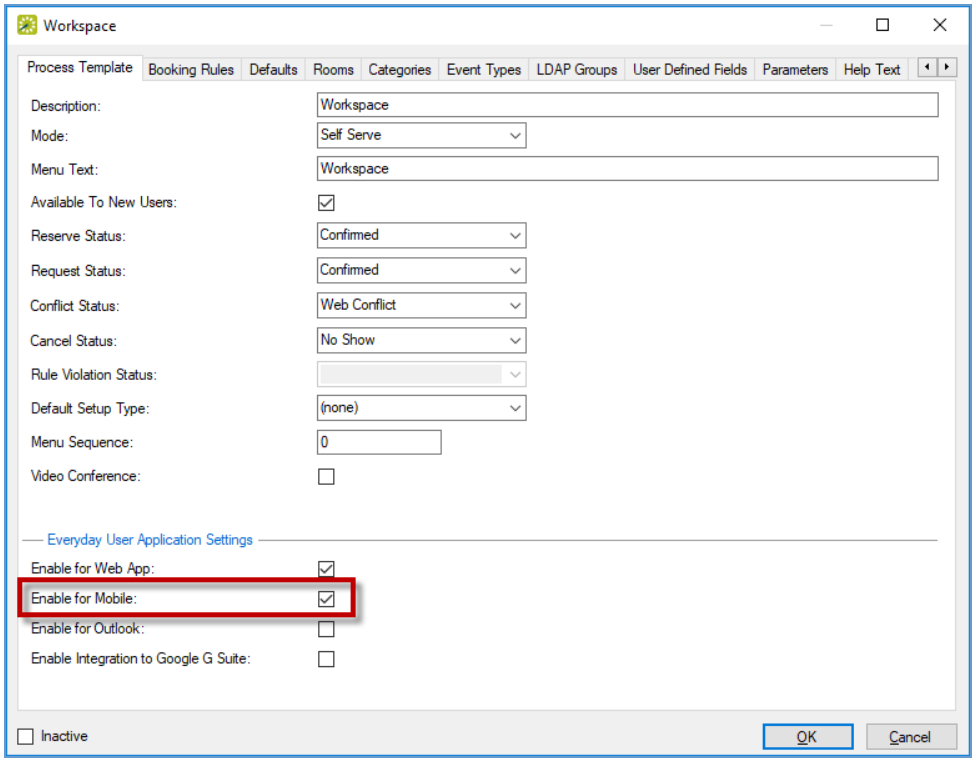
CHAPTER 23: Assign Templates to EMS Mobile App Users

EMS V44.1 allows you to select which Everyday User Process Template (e.g., "web process templates") will be enabled on your users' mobile devices.

1. In the EMS Desktop Client, navigate to **Configuration** > **Everyday User Applications** > **Everyday User Process Templates**.
2. Select the template you want to assign and click **Edit**.

> **Note:**
> If you do not yet have a process template, create one by clicking **New**. See Also: Configure Everyday User Process Templates.

3. An Everyday User Process Template dialog box will appear. Check the **Enable for Mobile** checkbox on the first tab of the template dialog box:



Note:

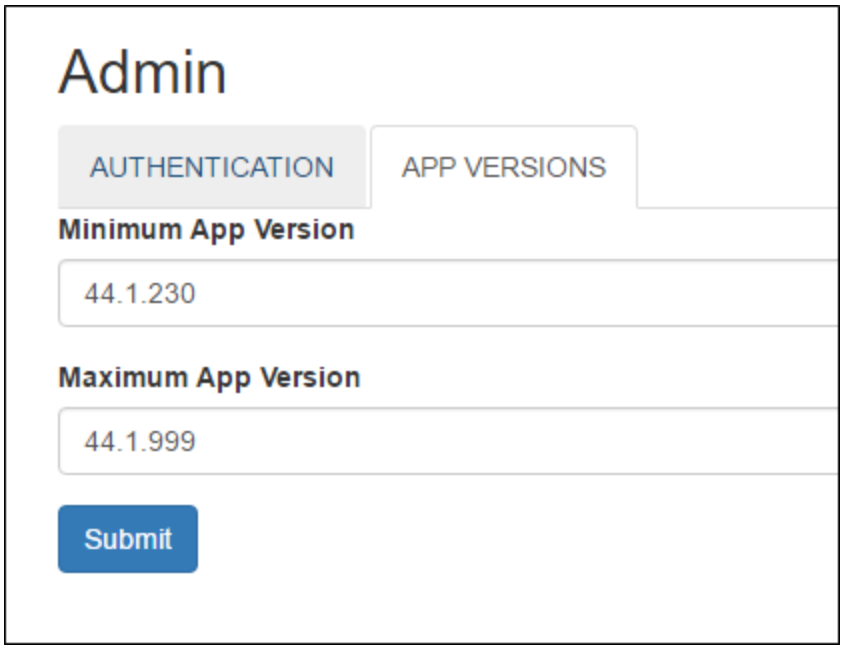
EMS Mobile Appis designed to make and edit simple reservations for users "on the go." At this time it cannot handle service requests, video conference bookings or complex workflows. Please consider this when you decide which templates should be enabled for the EMS Mobile App. Additionally, you can only change the name and icon of the EMS Mobile App through private deployment via MDM. Please refer to your MDM guide for instructions on how to change the name and icon of the EMS Mobile App.

CHAPTER 24: Restrict Users' EMS Mobile App Versions

Starting with the August 2016 release, EMS will ensure that EMS Mobile App is both forwards- and backwards-compatible, so that the EMS Mobile App will still function even if users update it on their devices. Alternatively, if you update your API but users do not update their app, functionality remains intact.

You might want to force users to keep their installations up to date. For example, you might want them to upgrade their EMS Mobile App after you upgrade the API, or you might want to prevent them from updating their EMS Mobile App until you upgrade the API. To enforce these restrictions, follow the steps below.

1. Log in to the API admin page (previously configured here).
2. Click on **Admin** tab, and set the minimum and maximum app versions:



Determine EMS Mobile API and Version Compatibility

Use the matrix below to determine how you want to enforce user updates.

EMS Release #	Mobile App Version Shipped	Mobile API Version	Mobile App Minimum Version	Mobile App Maximum Version
V44.1	44.1.241	44.1.129	44.1.238	44.1.241
V44.1	44.1.288	44.1.146	44.1.288	44.1.288

EMS Release #	Mobile App Version Shipped	Mobile API Version	Mobile App Minimum Version	Mobile App Maximum Version
Update 1				
V44.1 Update 2	44.1.319	44.1.158	44.1.288	44.1.319
V44.1 Update 3	44.1.410	44.1.172.0	44.1.288	44.1.410
V44.1 Update 4	44.1.430	44.1.187.0	44.1.288	44.1.430
V44.1 Update 5	NA	NA	NA	NA
V44.1 Update 6	44.1.477	44.1.208.0	44.1.288	44.1.477
V44.1 Update 7	44.1.487	44.1.249.0	44.1.288	44.1.487

Note:

The Minimum App Version means that users running EMS Mobile App below the minimum will not be able to use EMS. Increasing this value essentially forces users on an older version to upgrade. Maximum App Version prevents users from using EMS Mobile App if they run a version above the max.

CHAPTER 25: Change the Help Link Label and URL

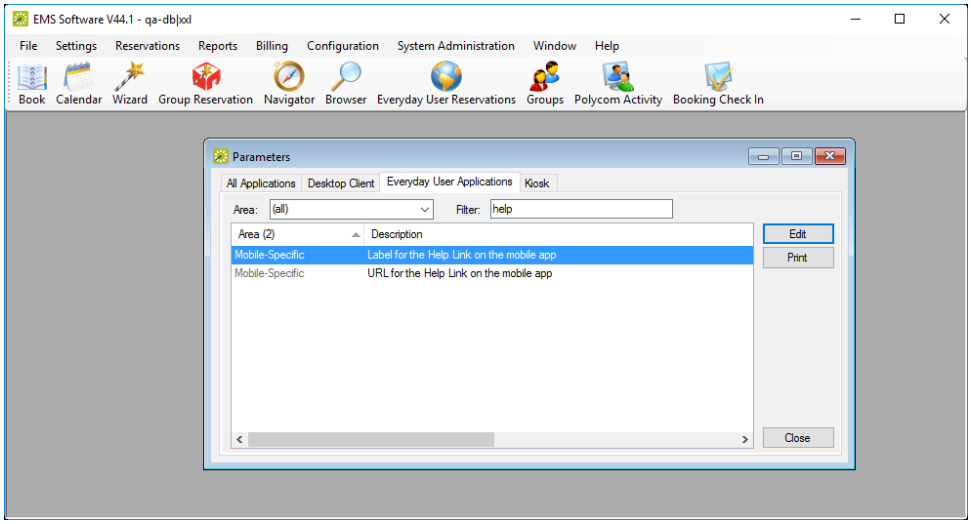
Admins can customize both the Label for the Help Link and the URL for the Help Link on the EMS Mobile App.

This topic provides information that will allow you to:

- Change the Label for the Help Link on the EMS Mobile App
- Change the URL for the Help Link on the EMS Mobile App

Change the Label for the Help Link

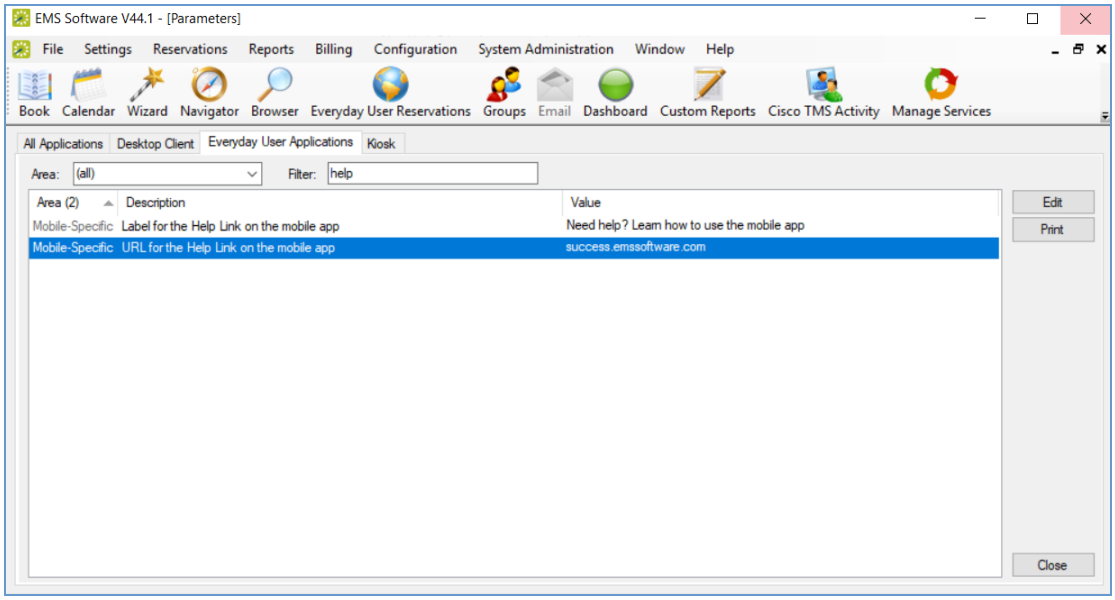
1. Locate the Everyday User Applications parameter, **Label for the Help Link on the mobile app.**
2. Enter a new value.



See Also: EMS Mobile App Parameters.

Change the URL Help Link

1. Locate the parameter, **URL for the Help Link on the mobile app**.
2. Enter a new URL.


EMS Software V44.1 - [Parameters]
File
Settings
Reservations
Reports
Billing
Configuration
System Administration
Window
Help
Book
Calendar
Wizard
Navigator
Browser
Everyday User Reservations
Groups
Email
Dashboard
Custom Reports
Cisco TMS Activity
Manage Services
All Applications
Desktop Client
Everyday User Applications
Kiosk
Area:
(all)
Filter:
help
Area (2)
Description
Value
Mobile-Specific
Label for the Help Link on the mobile app
Need help? Learn how to use the mobile app
Mobile-Specific
URL for the Help Link on the mobile app
success.emssoftware.com
Edit
Print
Close

CHAPTER 26: Configure EMS Mobile App QR Codes

In order to associate rooms with QR Codes, System Administrators must run and print a Room Card - QR Code report (under Hoteling) in the EMS Desktop Client. This automatically generates the codes and associates them with the designated rooms.

See Also: Scan QR Codes in the EMS Mobile App and Configure and Generate Room QR Codes.

CHAPTER 27: How Do I Know When to Upgrade the EMS Mobile App and API?

Determine EMS Mobile API and Mobile App Version Compatibility

Use the matrix below to determine how you want to enforce user updates.

EMS Release #	Mobile App Version Shipped	Mobile API Version	Mobile App Minimum Version	Mobile App Maximum Version
V44.1	44.1.241	44.1.129	44.1.238	44.1.241
V44.1 Update 1	44.1.288	44.1.146	44.1.288	44.1.288
V44.1 Update 2	44.1.319	44.1.158	44.1.288	44.1.319
V44.1 Update 3	44.1.410	44.1.172.0	44.1.288	44.1.410
V44.1 Update 4	44.1.430	44.1.187.0	44.1.288	44.1.430
V44.1 Update 5	NA	NA	NA	NA
V44.1 Update 6	44.1.477	44.1.208.0	44.1.288	44.1.477
V44.1 Update 7	44.1.487	44.1.249.0	44.1.288	44.1.487

Note:

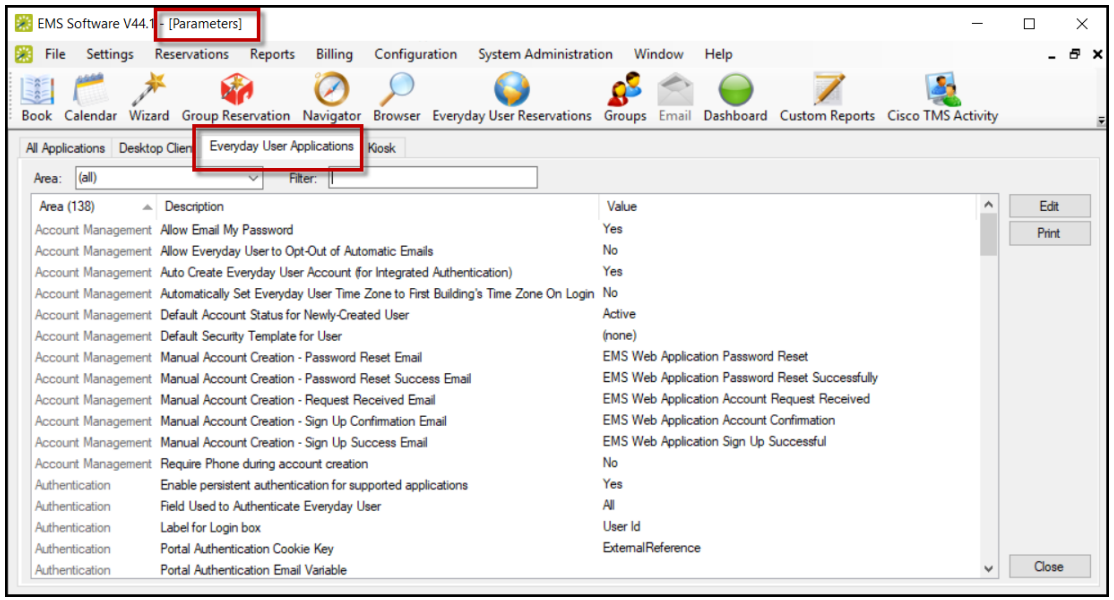
"*Minimum app version*" means that users running EMS Mobile App below the minimum will not be able to use EMS. Increasing this value essentially forces users on an older version to upgrade. "*Maximum app version*" prevents users from using EMS Mobile App if they run a version above the max.

CHAPTER 28: EMS Mobile App System Parameters

Parameters for the EMS Mobile App are configured in the EMS Desktop Client.

1. To access these parameters navigate to **System Administration** > **Settings** > **Parameters** > Everyday User Applications tab.
2. Under the Area dropdown, choose **Mobile Specific**.

> **Note:**
> Parameters for Exchange Integration Web Service and LDAP can be found by navigating to **System Administration** > **Settings** > **Parameters** > Desktop Client tab.



Parameters for the EMS Mobile App

Mobile App Parameters

The table below provides the titles, descriptions, values, and examples for EMS Mobile App parameters.

Area	Title	Description	Value	Example
Mobile-Specific	Field to find rooms by when scanning QR codes	Indicates the fields you want to match rooms by Room ID, Room Code or External Reference.	Room ID, Room Code, External Reference (on room).	

Area	Title	Description	Value	Example
Mobile-Specific	Label for the Help Link on the Mobile App	Login to the EMS Mobile App and click on top left navigation bar. On the bottom there is a help URL. This parameter allows you to configure the label for the help link. You can also configure the URL using another parameter - URL for HELP link on the EMS Mobile App.		Login to the EMS Mobile App and click on top left navigation bar. On the bottom there is a help URL.
Mobile-Specific	Maximum EMS Mobile App version that the API should allow to connect.	Maximum app version that the API will allow to connect.		
Mobile-Specific	Minimum EMS Mobile App version that the API should allow to connect.	Minimum app version that the API will allow to connect.		
Mobile-Specific	Minimum number of minutes to book via QR code or mobile Browse Location			
Mobile-Specific	Mobile check-in proximity distance			
Mobile-Spe-	Mobile proximity unit			

Area	Title	Description	Value	Example
cific	of measurement			
Mobile-Specific	Scans custom QR codes and interprets them as URLs.	QR Codes when scanned, can be configured to be interpreted as a URL. If the Customer's configuration requires QR codes to be scanned as a URL, this parameter should be set to YES. If set to No, QR Codes will be scanned as plain text.		
Mobile-Specific	Sets the header variable for the EMS Mobile APIs Header Authentication Method	EMS Mobile App supports header authentication. The value of the header variable is set on the Platform's Admin page. The same value should also be set for this parameter to make the Header Authentication work.		See Also: Portal Authentication Methods.
Mobile-Specific	The Query String Field in QR Code URLs for looking up Rooms	If you have the parameter SCAN CUSTOM QR CODES and INTERPRETS THEM AS URLS set to YES, then this is what tells the app to look for in the Query string.		If set to ROOMID, when it goes to the following URL: http://b-lah.com?romID=23921, it would use that ROOMID to look up the room based on the parameter: FIELD TO FIND ROOMS BY WHEN SCANNING QR CODES.
Mobile-Specific	The subject for the EMS Mobile two-	Subject of the email sent to users notifying them to go to the EMS Web App and scan		The first time you configure 2fa (Two-Factor Authentication)

Area	Title	Description	Value	Example
	factor setup email	their 2fa barcode.		you get e-mailed. This is the subject of that e-mail.
Mobile-Specific	URL for the EMS Mobile App in the app store	Setting this parameter to blank prevents the EMS Mobile App popup prompt from appearing.		
Mobile-Specific	URL for the EMS Mobile App in the play store	Setting this parameter to blank prevents the EMS Mobile App popup prompt from appearing.		
Mobile-Specific	URL for the Help Link on the mobile app	Login to the EMS Mobile App and click on top left navigation bar. On the bottom there is a help URL. The URL you put here, will be the URL for the Help Link. You can also configure the Help Link Label using another parameter - URL for HELP link Label on the EMS Mobile App.		

CHAPTER 29: EMS Mobile App User Guide

The EMS Mobile App, available for iOS and Android smartphones, is designed primarily for everyday users "on the go." The app allows users to make simple reservations in unmanaged spaces, such as workspaces and open conference rooms.

This user guide provides the following information about the EMS Mobile App:

Contact Customer Support

- **Option 1 (Recommended):** Search the Knowledge Base available at Accruent Access.
- **Option 2:** Submit a case directly via Accruent Access.
- **Option 3:** Email emssupport@accruent.com.
- **Option 4:** Phone (800) 288-4565.

Important!

If you do not have a customer login, register here.

CHAPTER 30: Introduction

EMS Mobile Appenables 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.

With the EMS Mobile App, Everyday Users can:

- Reserve a workspace from anywhere, at anytime
- Book a meeting and invite attendees
- Update details of an existing booking
- Check-in to or cancel an upcoming meeting
- Swipe or scan a QR code to book or check in to a room or workspace
- Add or join a Skype for Business meeting with one click

For more information on new features and updates to the EMS Mobile App, see also: What's New and EMS Mobile App Release Notes.

Note:

Get up to speed fast using our EMS Mobile App Video Tutorials:

- Booking a Desk or Meeting
- Booking a Meeting By Scanning a QR Code

Note:

EMS also produces a more robust web-based application called **EMS Mobile Web**, which can be used on mobile devices. **See Also:** EMS Mobile Web App Versus EMS Mobile App: What's the Difference?

EMS Mobile enables you to manage space on mobile devices such as tablets and smartphones. Simple touchscreen gestures on mobile devices such as tablets and smartphones allow you to scan QR codes for rooms and to cancel, end, or check in to meetings

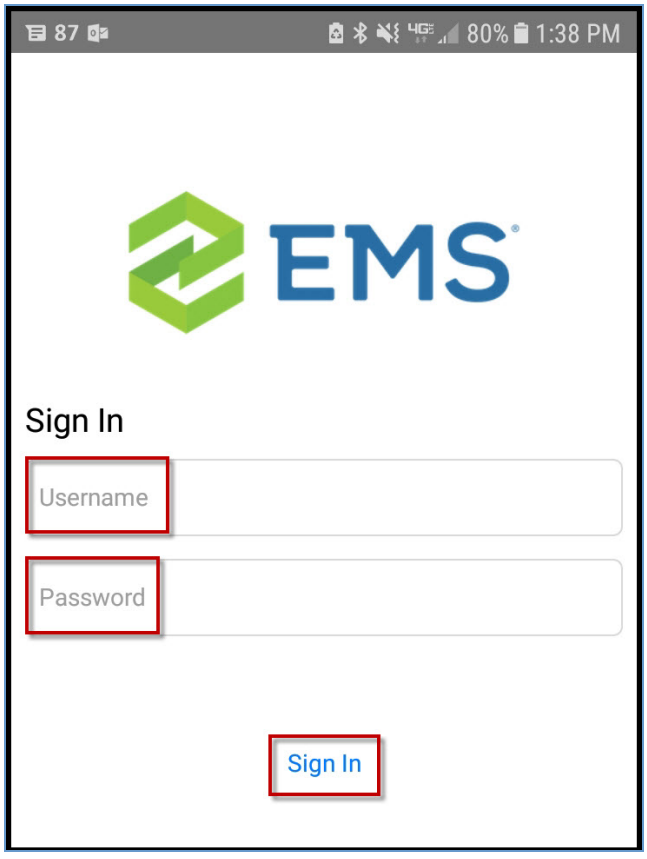
CHAPTER 31: Log In, Reset Password, or Create an Account

This section provides instructions on:

- Log In to the EMS Mobile App
- Reset Your Password
- Create an Account

Log In to EMS Mobile App

1. Enter your **Username**.
2. Enter your **Password**.
3. Click **Sign In**.



4. Click **About** to view the following information:
   - Change API URL
   - Version Information—includes version number, Metadata and API Version

- Location Services—indicates whether Location Services are enabled
- QR Code Scanner—indicates whether the QR Code Scanner is enabled
- Logs—If you have enabled logging in EMS Platform Services, you can view, clear, or copy logs
- Import SSO Configuration

Reset Your Password

1. If you've forgotten your password, navigate to the **Sign In** page and click the **I've forgotten my password** link.
2. Provide your **username**:
   - If the username is in the EMS system, an email will be sent to the corresponding email address containing reset password instructions.
   - If the username is not in the EMS system, you will receive an error message and no reset instructions will be sent via email.

Create an Account

> **Note:**
> The Create Account link displays only if your Administrator has enabled it and your EMS Mobile App has retained the EMS Native authentication. The **Create Account** option is not available for Windows, LDAP, and SSO authentications.

1. Click the **Create Account** link at the bottom of the **Sign In** screen.
2. You will be asked to provide:
   a. Email Address
   b. Password
   c. Re-enter Password
   d. EMS Server URL
   e. Name
   f. Phone 1
   g. Time Zone
   h. Additional Details
   i. Accept the Terms of Use and Create Account
3. Click **Create Account**.

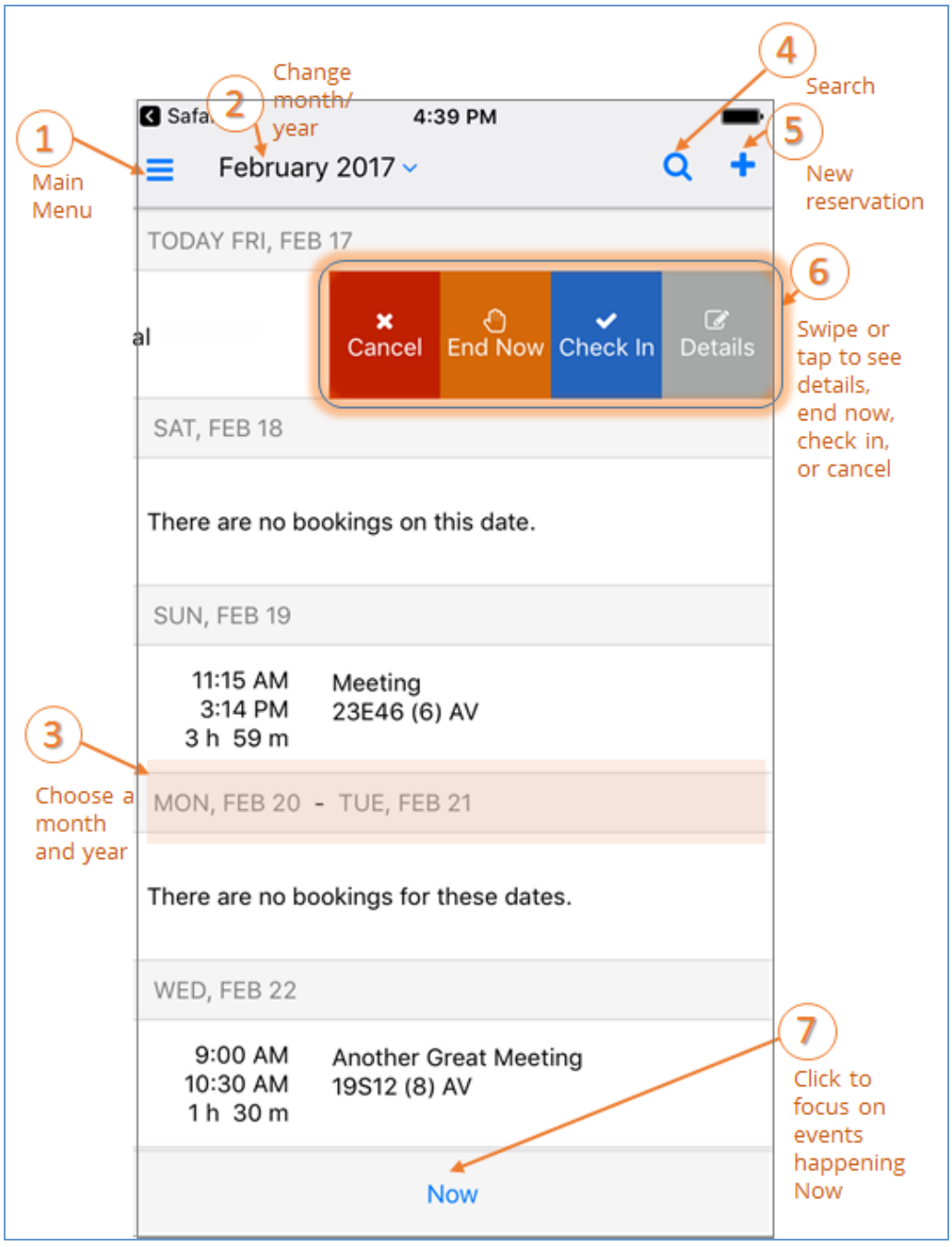
CHAPTER 32: Get Started with EMS Mobile App

Once you have downloaded the EMS Mobile App onto your phone, you can log in and begin using the app. Refer to the following topics for information on getting started:

- Log In, Reset Password, or Create an Account
- Enter Your Server URL
- Search for Meetings
- Check In to Meetings
- Cancel Meetings
- End Meetings Early
- Assign or Remove Favorite Locations
- Use QR Codes

Quick Start

Follow the tips in the image below to interact with your calendar and see your events. Your calendar shows only current and upcoming events.



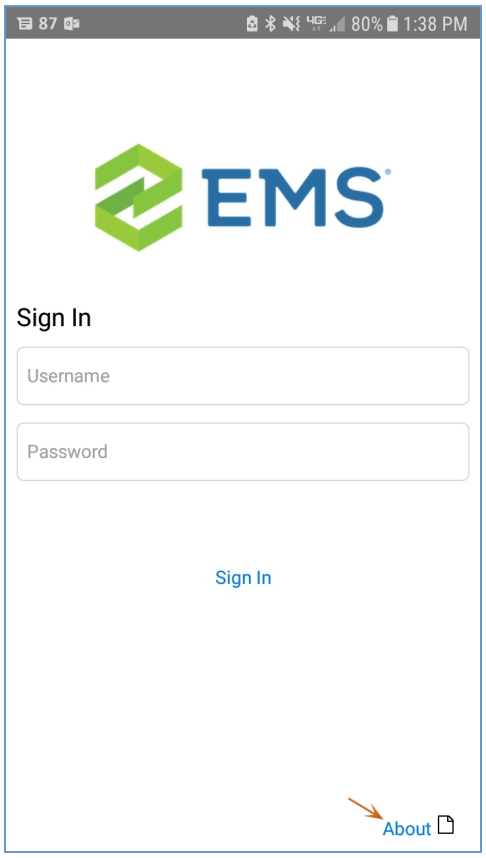
Home Screen, EMS Mobile App

CHAPTER 33: Enter Your Server URL

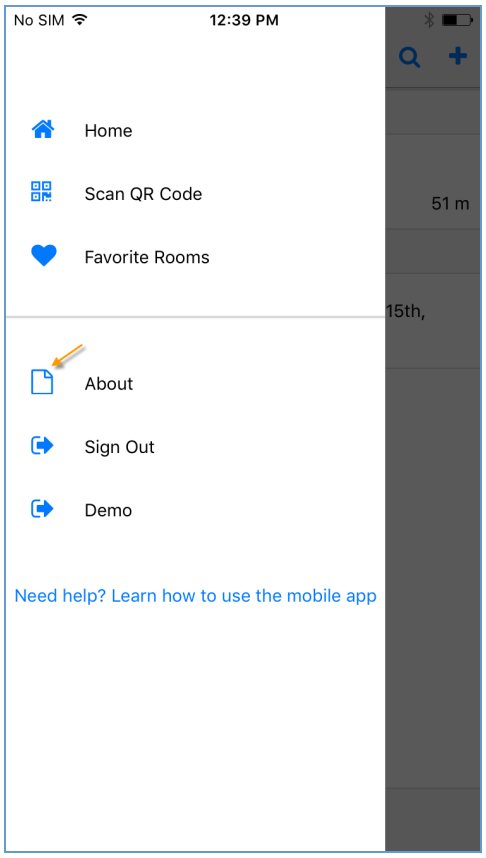
You can view and change the Server URL (also referred to as the API URL) to which your EMS Mobile App points.

To view or change the Server URL, do the following:

1. From the **Sign in** screen, tap **About** in the lower right-hand corner, or after signing in, tap on the menu and navigate to the **About** screen.

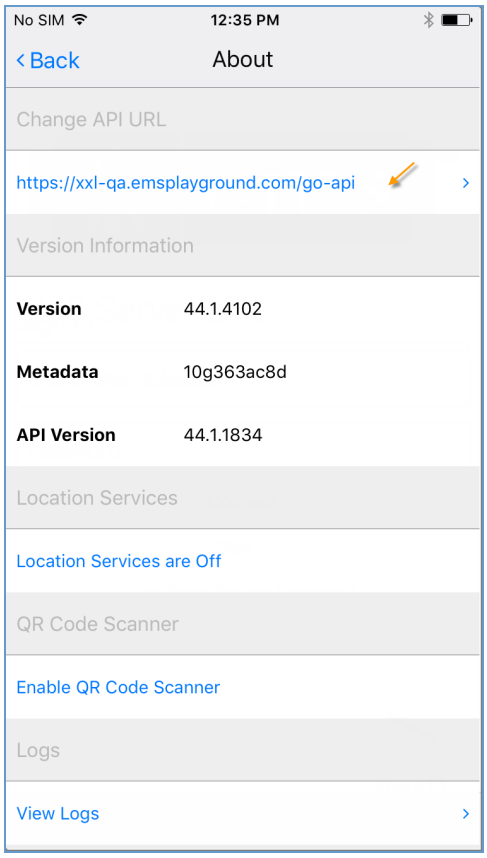


Tab About from Sign In Screen

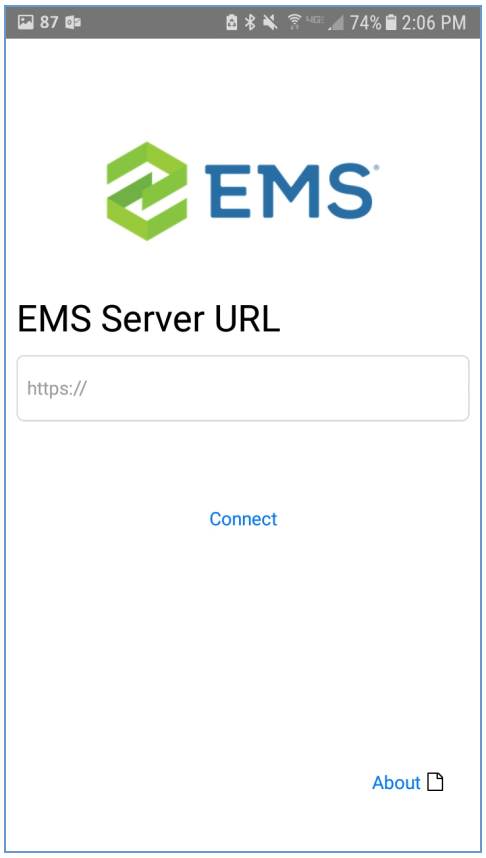


Tap About from Main Menu

2. From the About screen, the API URL is listed under Change API URL. To change the API URL, tap the API URL address. The Server URL screen will appear.

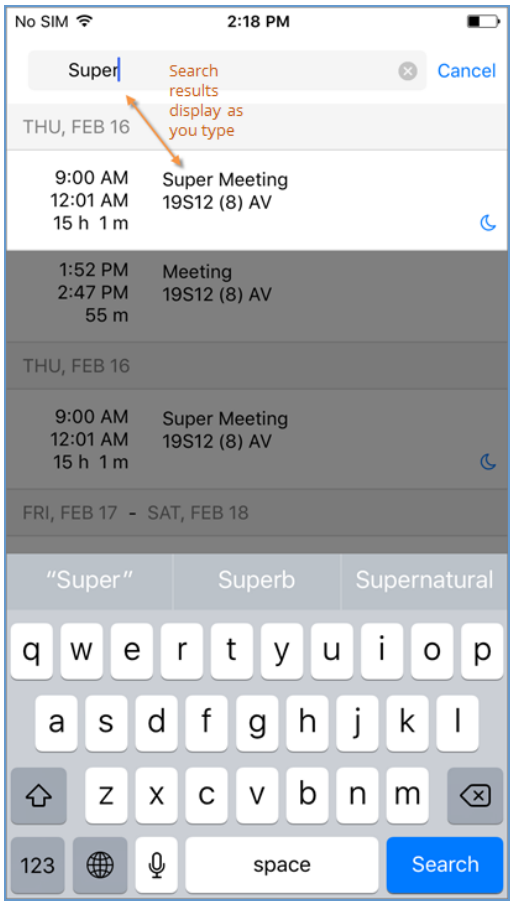


3. Enter your server URL in the field and tap **Connect**. Check with your Administrator for the correct URL.


87
74% 2:06 PM
EMS
EMS Server URL
https://
Connect
About

CHAPTER 34: Search for Events

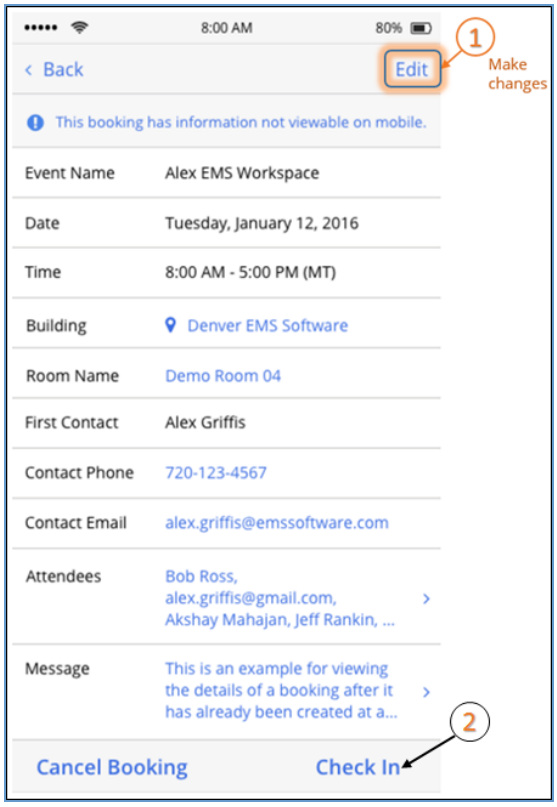
To search for existing events, Tap the Search icon and enter a keyword in the Search field.



CHAPTER 35: Check In to Meetings

You can check in to an event in one of two ways:

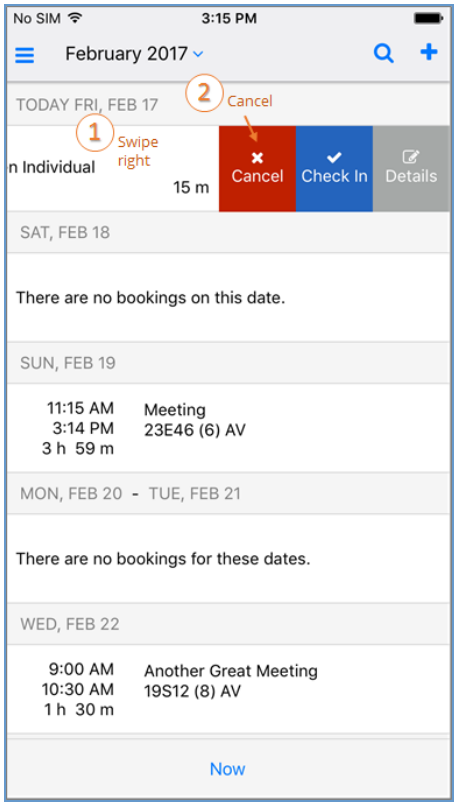
1. From the Calendar on the **Home** page, locate the event you want to check in to.
    a. If it is within the pre-determined check-in time period, a **Check In** option will appear when you swipe right. The meeting organizer or booking template determines how soon in advance of a meeting you can check in.
2. You can also Check In by opening and/or editing an event.
    a. Tap on the event and click **Edit** in the upper right-hand corner.
    b. Click **Check In**.



CHAPTER 36: Cancel a Meeting

You can cancel an existing meeting in one of two ways:

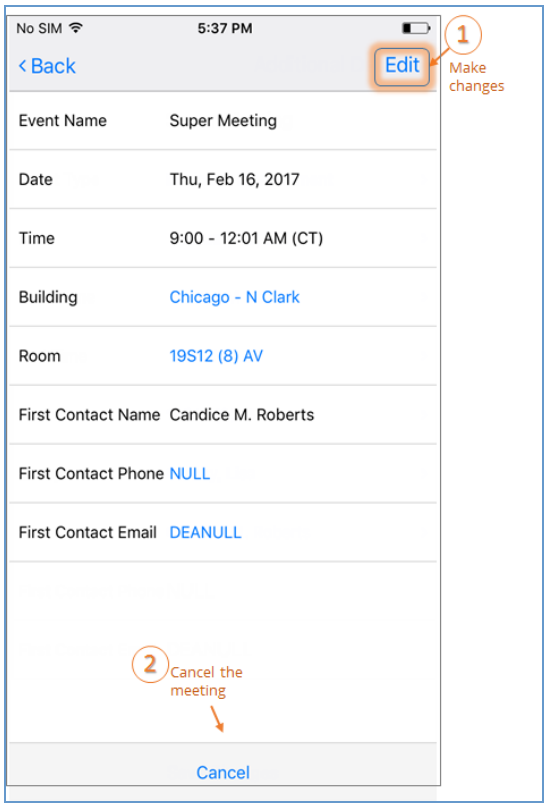
1. From the Calendar on the **Home** page, locate the meeting you want to cancel.
    - If you are able to Cancel the meeting, a **Cancel** option will appear when you swipe right. The meeting organizer or booking template usually determines your permissions control and whether you can cancel a meeting. If enabled, attendees will be notified.



Accessing the Cancel Option

2. You can also Cancel by opening and/or editing an event.
   - Tap on the event and click **Edit** in the upper right-hand corner. Click **Cancel**.

> **Note:**
> If your meeting has taken less than the reserved time, you can End a meeting early to release the space for others. See Also: End a Meeting Early.



Cancel an Event Through Edit Screen

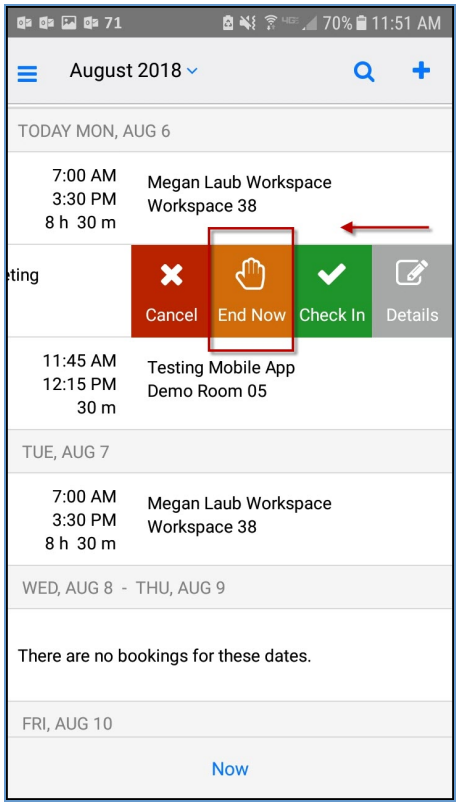
CHAPTER 37: End a Meeting Early

If your meeting has taken less than the reserved time, you can End a meeting Now to release the space for others.

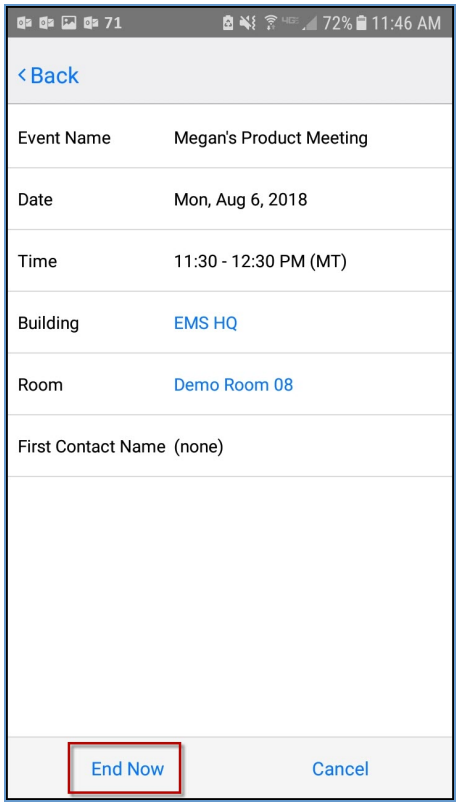
You can End a Meeting early in one of two ways:

1. From the Calendar on the Home Page:
    a. Locate the meeting on the Calendar that you want to **End Now** and swipe left.
    b. If you are able to end the meeting, an **End Now** option will appear. The meeting organizer or booking template determines whether this option is available.

> **Note:**
> The End Now button will only appear on non–Exchange-enabled templates.



2. By editing the event:
    a. Tap on the event and click **Edit** in the upper right-hand corner.
    b. Click the **End Now** link in the lower left corner.



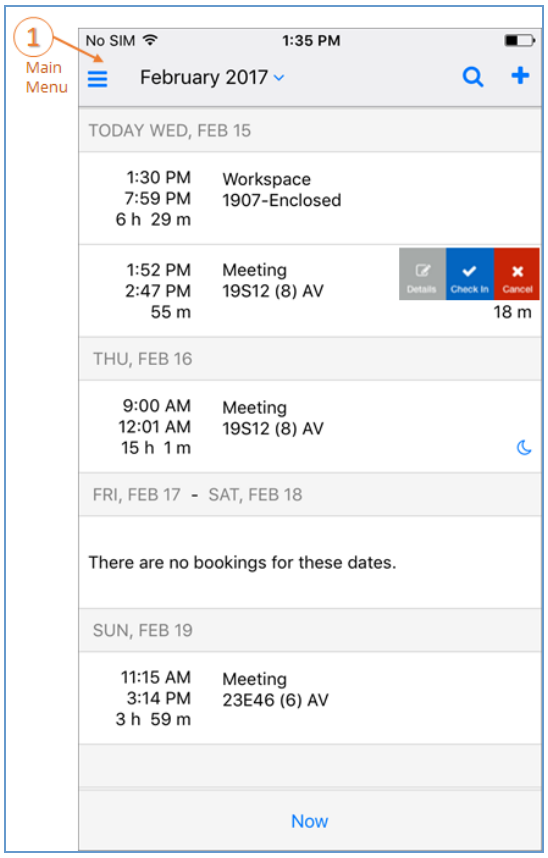
See Also: Invite People.

CHAPTER 38: Assign or Remove Favorite Locations

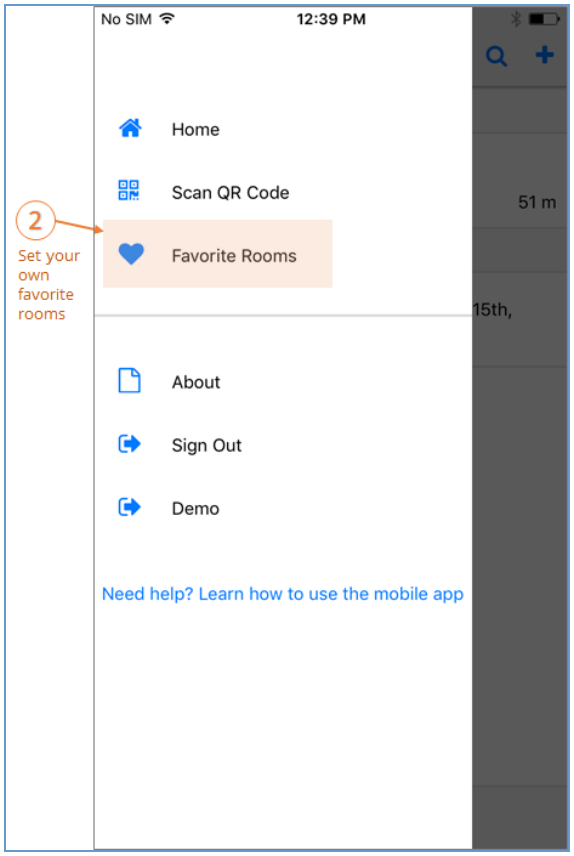
Assigning favorite locations streamlines the booking process and filters your location search results. This topic provides information on the following:

Assign a Location as a Favorite

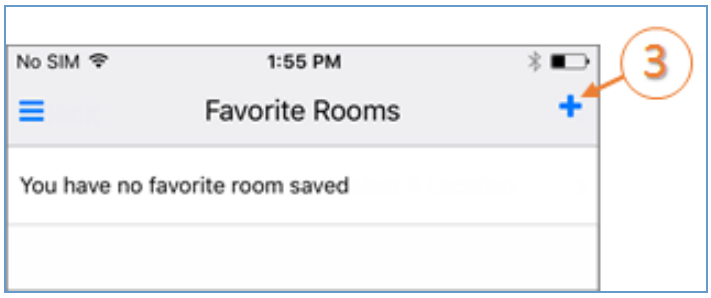
1. Tap the main menu icon in the upper left corner of the Home screen.



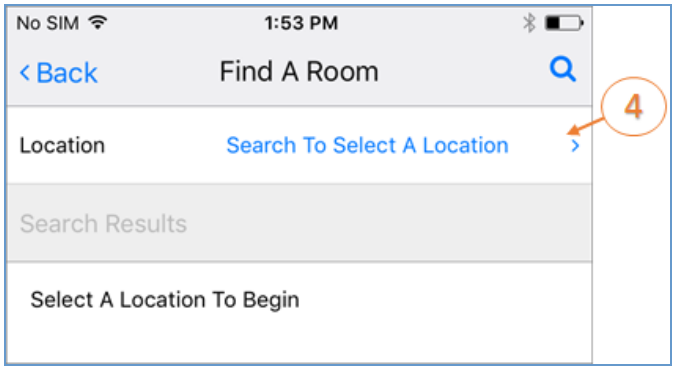
2. Tap **Favorite Rooms**.



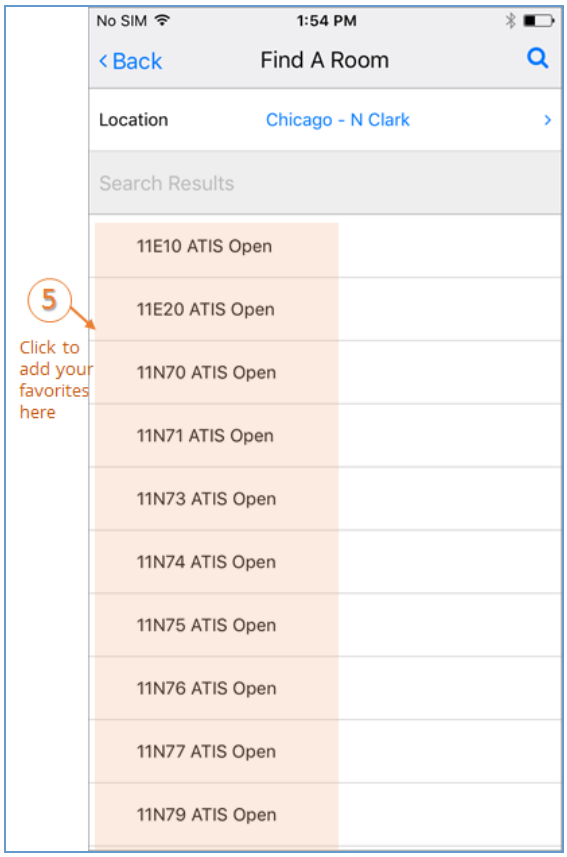
3. Click the **+** symbol to add a room to your list of Favorites.



4. The Find a Room screen will appear. Search for rooms by **Location**.



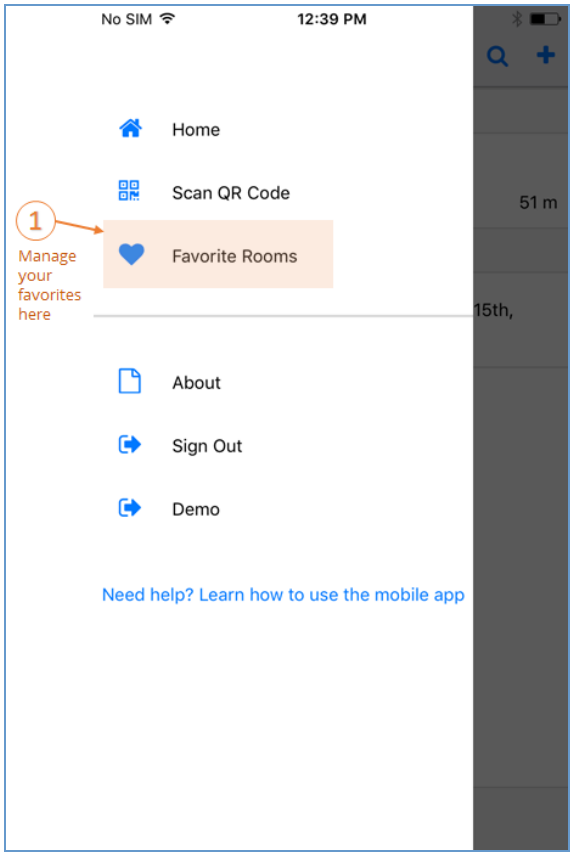
5. Choose a location from the Search Results list. When you search for locations during the booking process, those that are in your favorites list will be listed first.



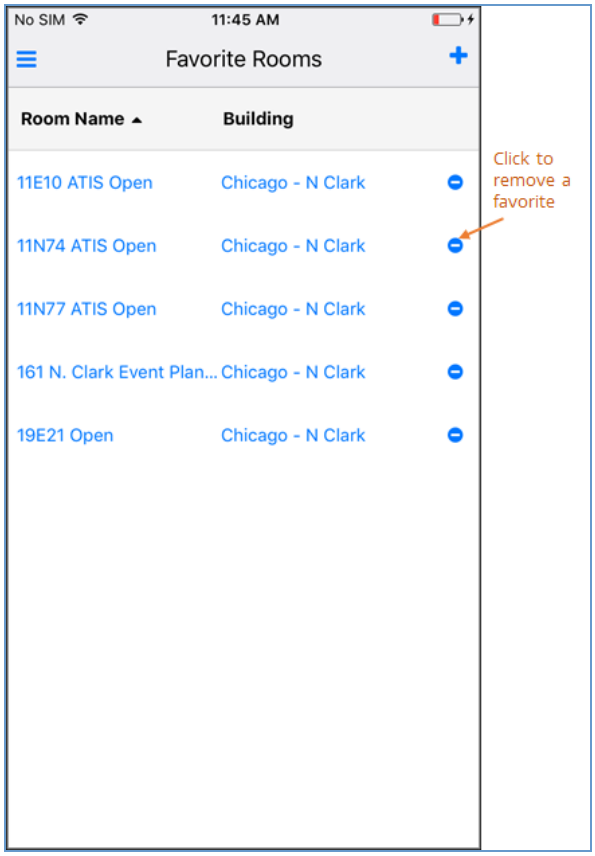
Remove a Favorite Location

When you no longer want to see a location listed first in search results, you can remove it from your personalized list.

1. Navigate to your Favorites list by clicking on the main menu in the upper left corner of EMS Mobile App and selecting **Favorite Locations**.



2. Click the **Remove** icon to remove a Favorite from your list.



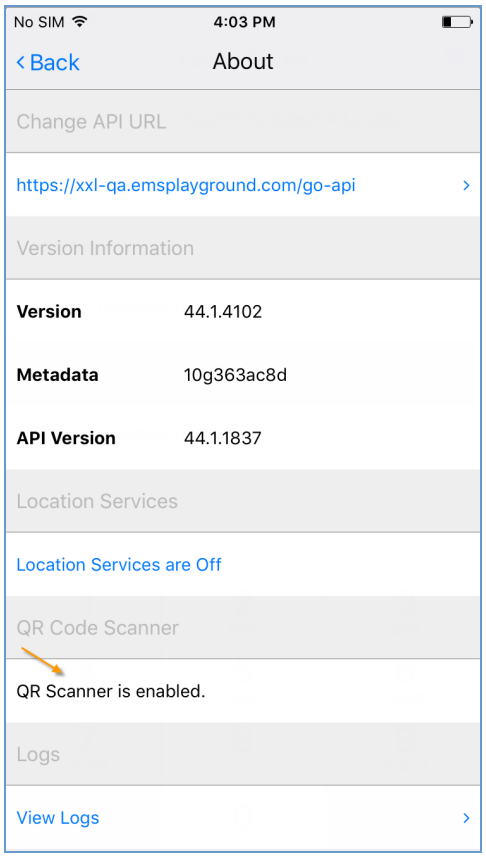
CHAPTER 39: Scan QR Codes in EMS Mobile App

The QR Code Scanner feature of EMS Mobile App allows you to easily create a new booking or check in to a meeting you are hosting.

To create a new booking using the QR Code Scanner:

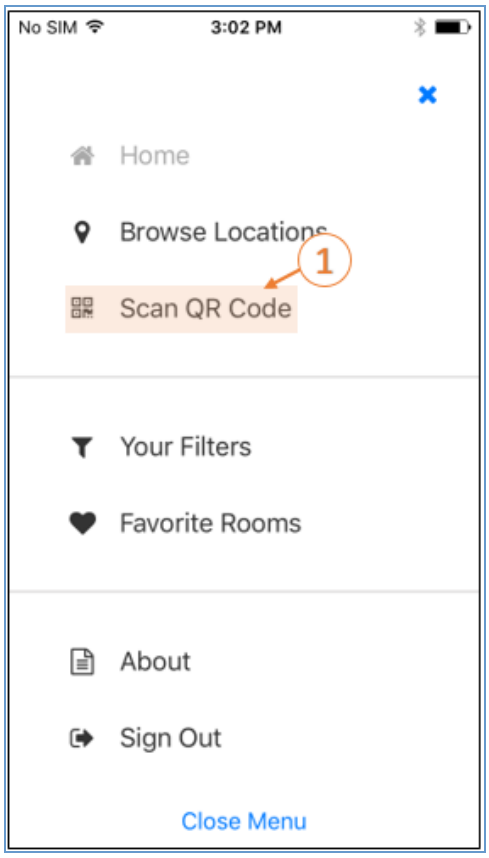
1. You must first enable this functionality by navigating to the **Main Menu** on the Mobile App and tapping **About**.

2. Navigate to the **QR Code Scanner** field and ensure that the QR Code Scanner is enabled.



QR Code Scanner Field

3. When you are ready to scan a QR Code using the EMS Mobile App, navigate to the **Main Menu** and tap **Scan QR Code**.



4. Scan the workspace QR Code. A new booking is created and will appear in your Calendar. From the EMS Mobile App, you can now:
   - Book the room immediately (based on availability) using your assigned booking template(s).
   - Check in to the meeting (if you are the host).

CHAPTER 40: Attend a Meeting

Any events you have been invited to appear on your Calendar on the Home Page of the EMS Mobile App.

Check In to a Meeting

Once you've logged in, you can check in to an event in one of two ways:

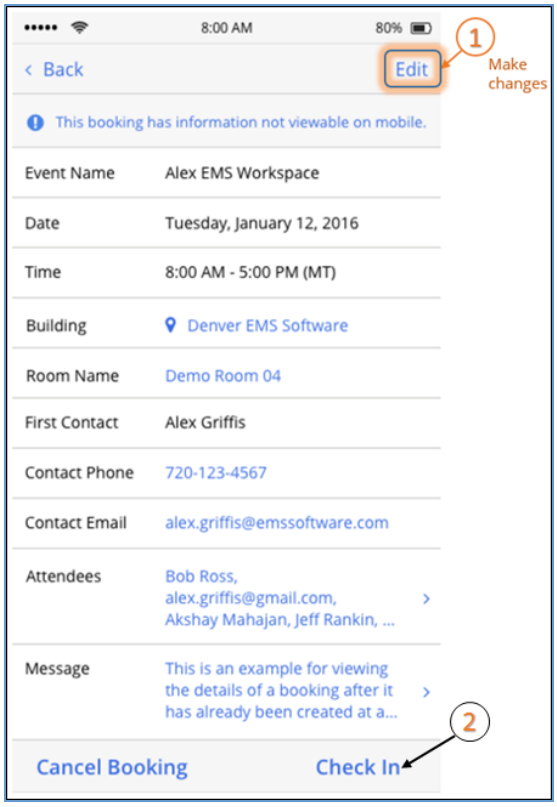
1. From the **Calendar** on the **Home** page, locate the event you want to check in to.

   If it is within the pre-determined check-in time period, a **Check In** option will appear when you swipe left. The meeting organizer or booking template usually determines how soon before a meeting you can check in.

2. You can also **Check In** by opening and/or editing an event.

   a. Tap on the event and click **Edit** in the upper right-hand corner.

   b. Click **Check In**.



See Also: Invite People.

CHAPTER 41: Create a Meeting

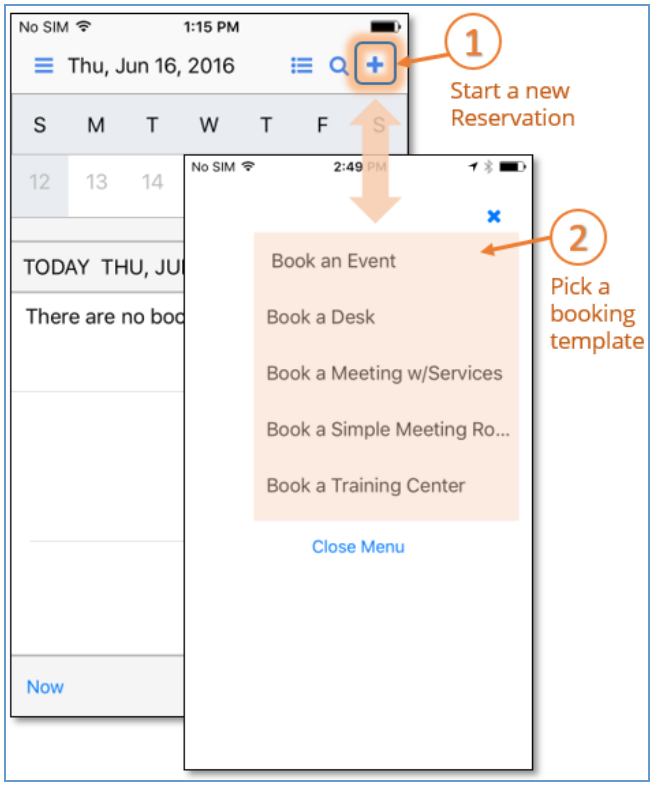
The EMS Mobile App allows users to quickly create bookings in un-managed spaces (or spaces without services and approvals), from the convenience of their mobile device.

This topic will provide information that will allow you to:

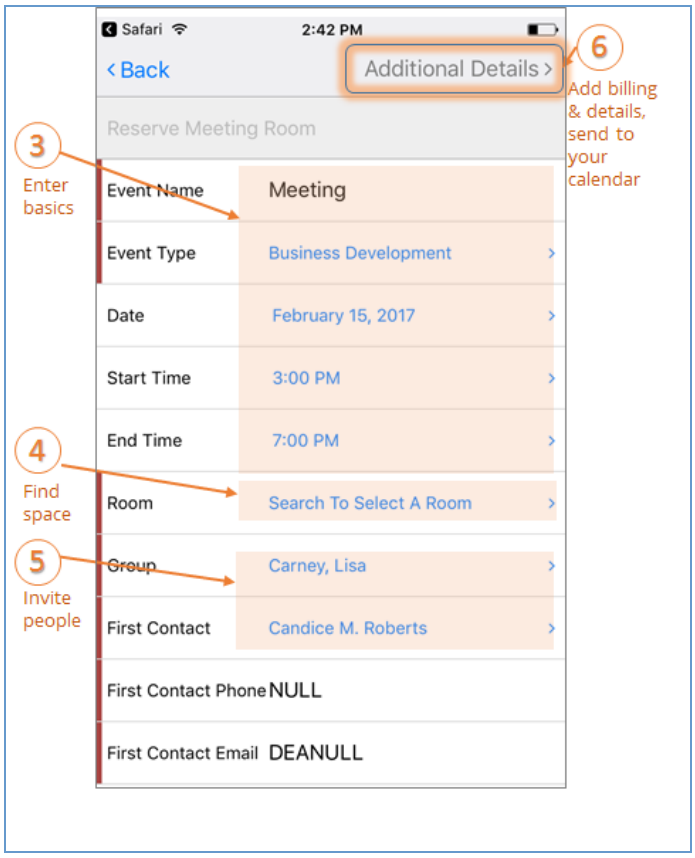
- Create a Booking Using the EMS Mobile App
- Search for a Room for Your Booking

Create a booking using the EMS Mobile App

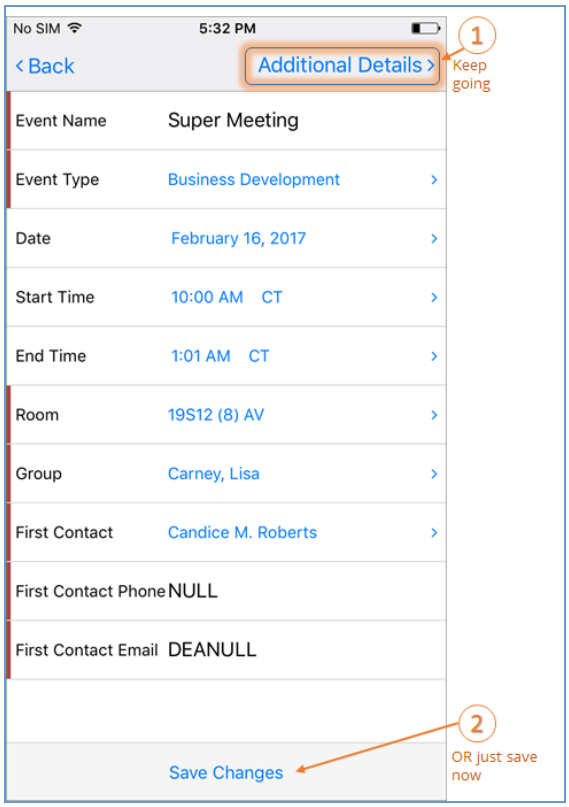
1. From the Calendar screen, tap the **New Reservation** (**+**) icon.
2. From the **Select A Template** screen, choose a booking template.



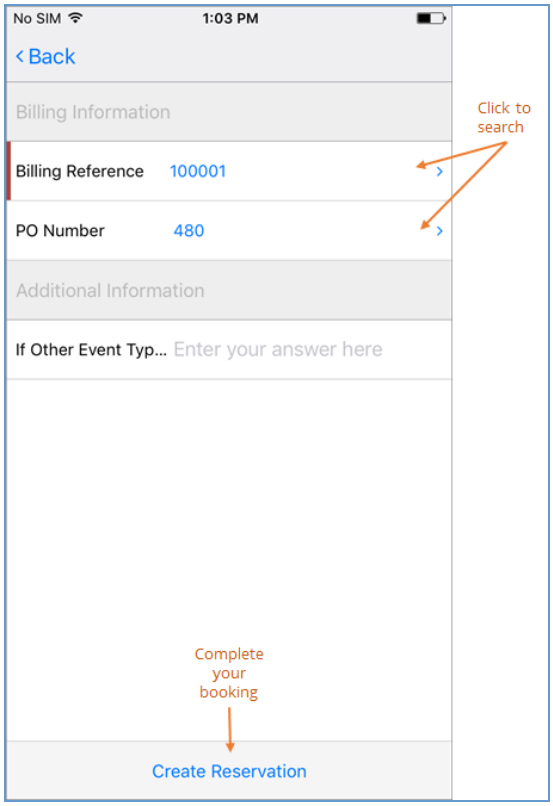
3. Enter the required information for your booking (**Event Name**, **Event Type**, Room, **Group**, and **First Contact**). Fields that appear here vary depending on your booking template.



d. Once you have selected a room and if the template allows, you can save and complete your reservation by clicking **Save Changes**. If the option is not available, continue to the next step.


No SIM
5:32 PM
Back
Additional Details
1
Keep going
Event Name
Super Meeting
Event Type
Business Development
Date
February 16, 2017
Start Time
10:00 AM CT
End Time
1:01 AM CT
Room
19S12 (8) AV
Group
Carney, Lisa
First Contact
Candice M. Roberts
First Contact Phone
NULL
First Contact Email
DEANULL
2
OR just save now
Save Changes

e. Click **Additional Details** to add billing and PO numbers and other information as required.

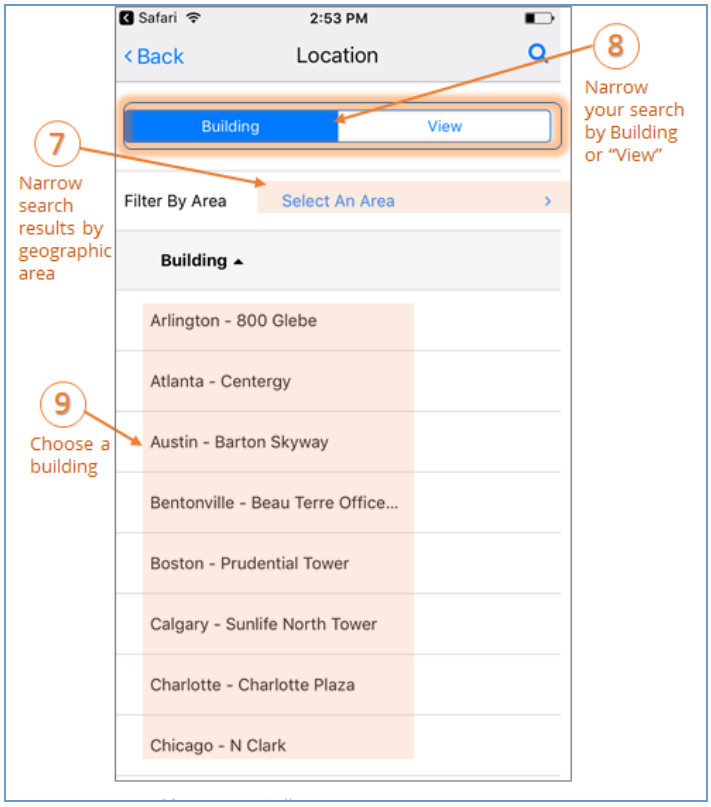


f. When all required information is complete and valid, click **Create Reservation** to finalize your booking and return to the Home page, where your reservation will appear in the calendar.

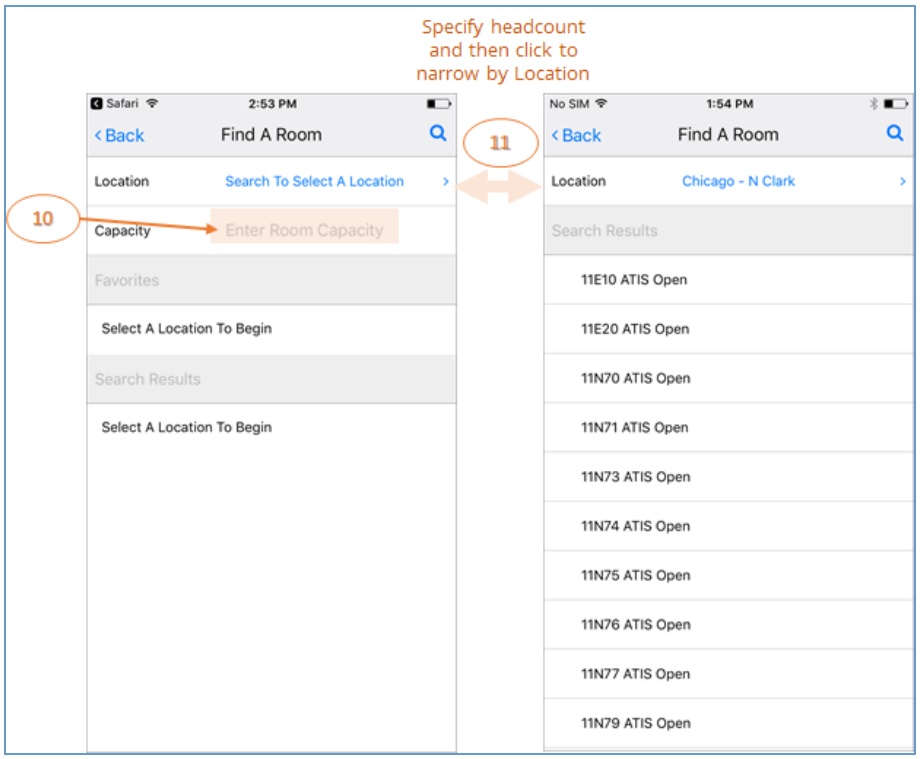
Search for a Room

1. During the booking process, search for a room by performing the following steps:
   a. On the New Reservation screen, click the **Room** field.
   b. On the **Find a Room** screen, search and filter your room criteria by:
      i. **Location**—the geographic or physical location of the space, such as a country, region, district, etc.
      ii. **Building**—the building in which the space is located.
      iii. **View**—the custom grouping your Administrator might have defined to pool and classify types of space, such as Offices, Conference Rooms, Classrooms, or Campuses.
      iv. **Area**—the area of a Building or View in which the space resides, such as floor, plaza, hall, or project.

c. Choose a **Building**.



d. Enter the numeric **Capacity** (total number of attendees) for your meeting to narrow Location search results. Rooms meeting your criteria will appear in the Search Results.

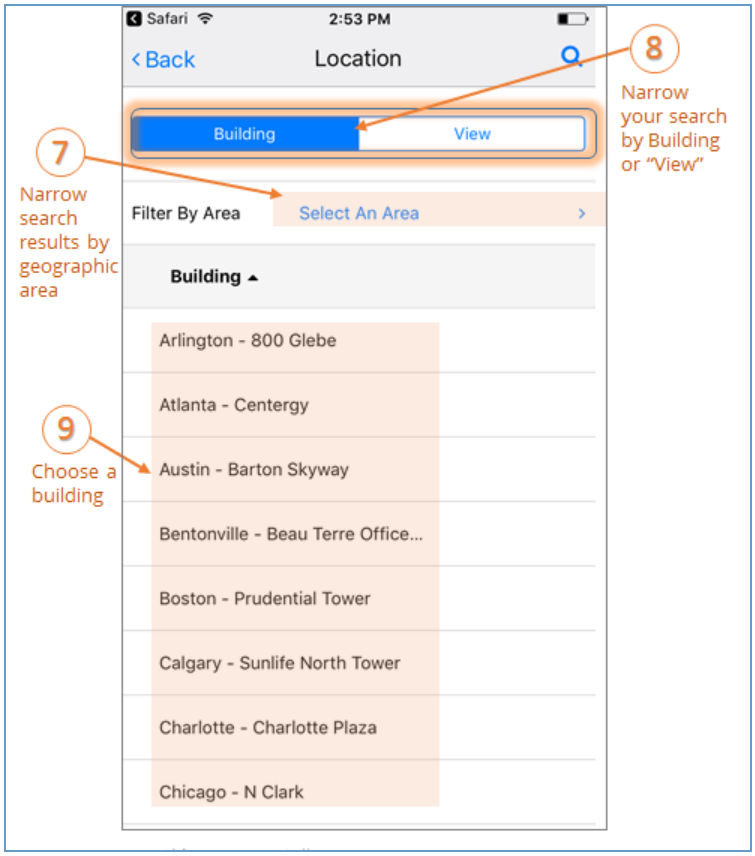


e. When you click to select a room for your meeting, you will be redirected to the booking page and the room you chose will now appear on your meeting.

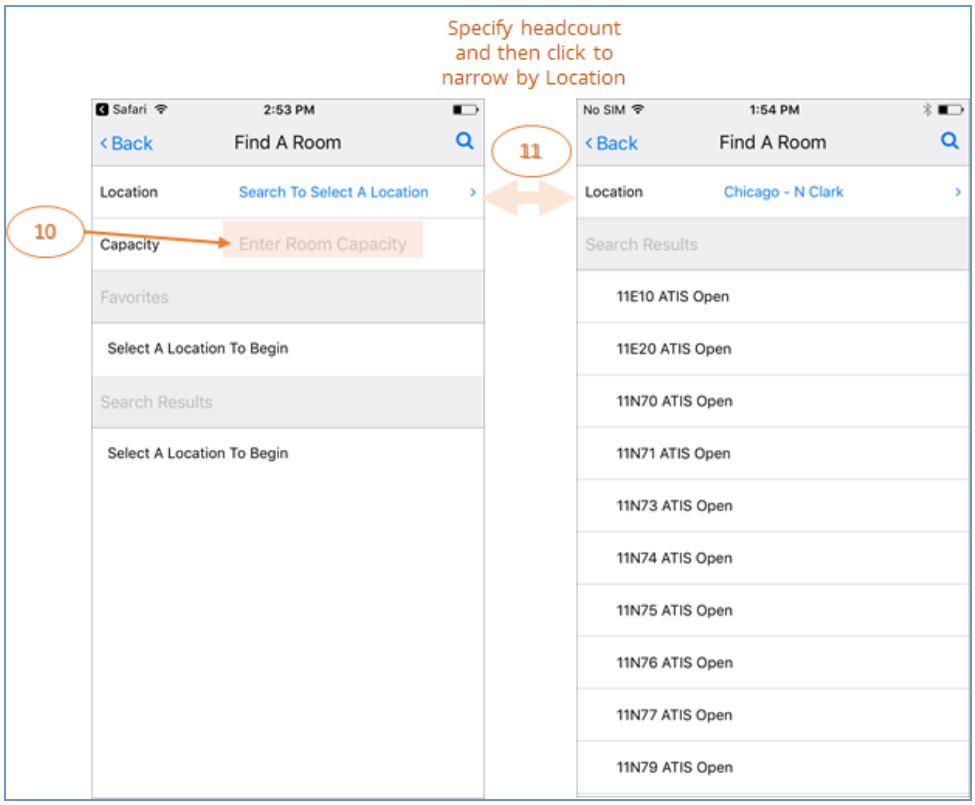
CHAPTER 42: Find a Room

Add a location to your booking by searching for and adding a room.

1. On the New Reservation screen, click the **Room** field.
2. On the Find a Room screen, search and filter your room criteria by:
   a. **Location** = the geographic or physical location of the space, such as a country, region, district, etc.
   b. **Building** = the building in which the space is located.
   c. **View** = the custom grouping your Administrator might have defined to pool and classify types of space, such as Offices, Conference Rooms, Classrooms, or Campuses.
   d. **Area** = the area of a Building or View in which the space resides, such as floor, plaza, hall, or project.
3. Choose a **Building**.



4. Enter the numeric **Capacity** (total number of attendees) for your meeting to narrow Location search results. Rooms meeting your criteria will appear in the Search Results.



5. When you click to select a room for your meeting, you will be redirected to the booking page, and the room you chose will now appear on your meeting.

CHAPTER 43: Invite People

When inviting people to your meetings, it is important to understand the difference between Attendees and Groups.

Concept: Groups and Attendees

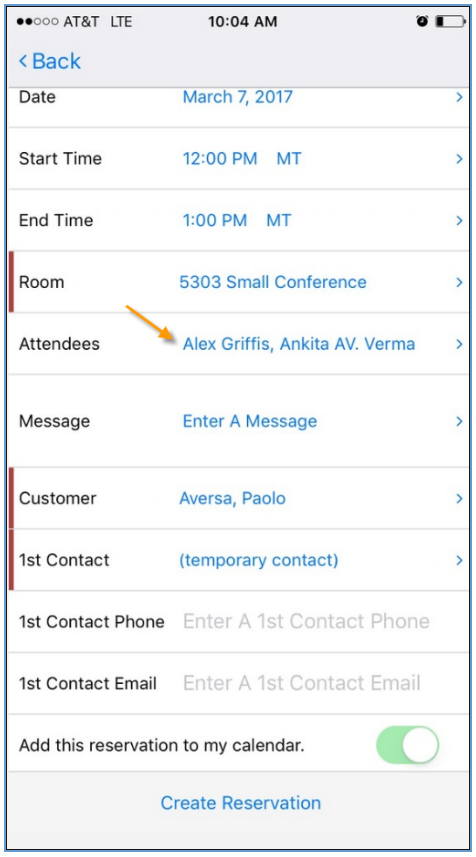
Attendees—Individuals who are invited to meetings (e.g., invitees).

A **Group**—The person(s) responsible for the meeting. Your Administrator sets the label for the Group field, so the name might vary (in the example below, it is labeled "Customer").

First Contact—A Group can designate a First Contact to oversee questions, changes, and updates to the meeting. (First Contacts are optional.) **First Contacts** will receive notifications regarding any meeting changes.

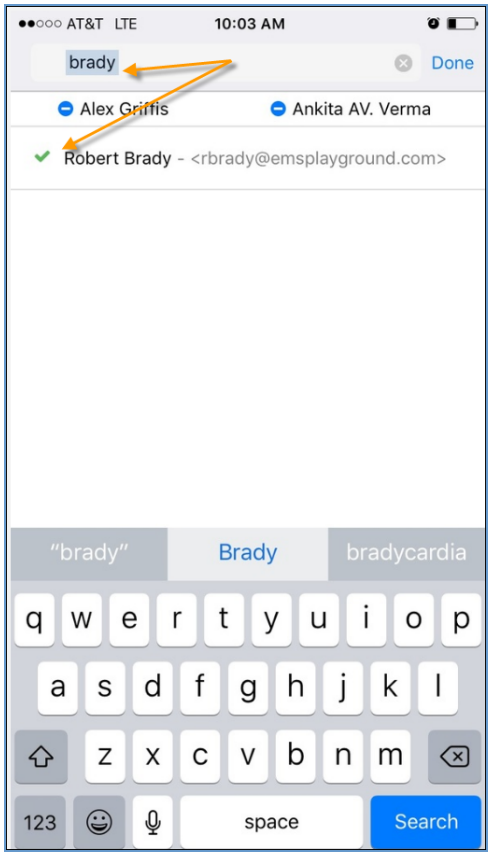
To invite people to your meeting:

1. During the booking process, tap the **Attendees** field to invite people to your meeting.

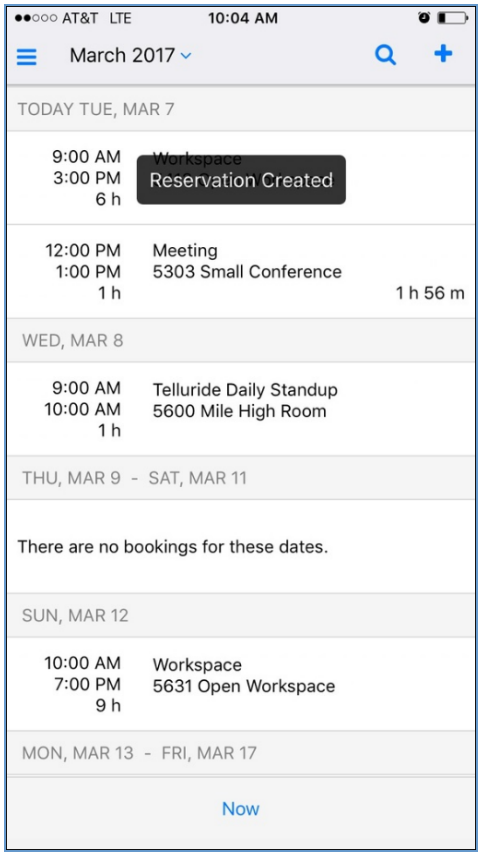


2. Search for people by entering name(s) in the **Search** field and tapping the Search icon. Tap on the names in the Search Results list to add them to the event. The list the system searches from is

defined by your Administrator.

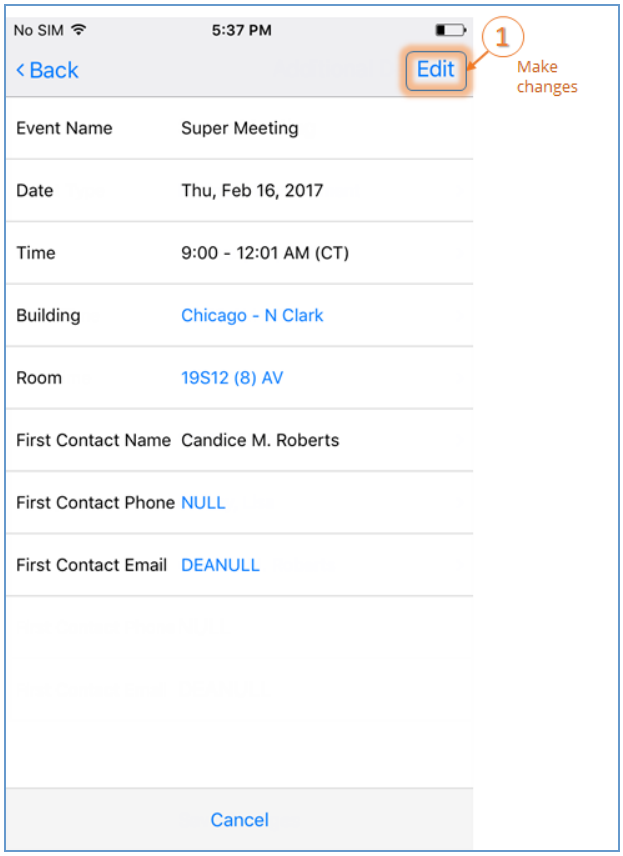


3. You might be able to add multiple attendees; invitees that are already on the meeting show at the top; you can remove them by tapping the blue **Remove** icon. Tap **Done** when finished.
4. In the **Message** field, enter the message you want to send about the meeting to attendees.
5. In the **Group** (or **Customer**) field, enter the name of the predefined group or person responsible for the meeting (on whose behalf you can book the meeting).
6. In the **First Contact** field (optional), enter the name of the person who will be the first point of contact for the meeting; they will receive notifications and updates about the meeting if details change.
7. Tap **Save** to complete the reservation. A message displays confirming that your reservation has been created. Your new booking will now appear on your Home page.


AT&T LTE
10:04 AM
March 2017
TODAY TUE, MAR 7
9:00 AM
3:00 PM
6 h
Workspace
Reservation Created
12:00 PM
1:00 PM
1 h
Meeting
5303 Small Conference
1 h 56 m
WED, MAR 8
9:00 AM
10:00 AM
1 h
Telluride Daily Standup
5600 Mile High Room
THU, MAR 9 - SAT, MAR 11
There are no bookings for these dates.
SUN, MAR 12
10:00 AM
7:00 PM
9 h
Workspace
5631 Open Workspace
MON, MAR 13 - FRI, MAR 17
Now

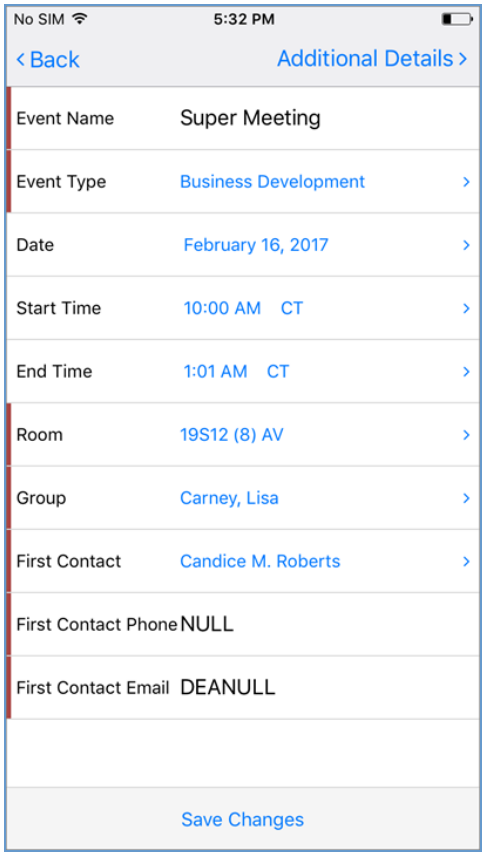
CHAPTER 44: Edit a Meeting

1. From your **Home** screen, tap on the event you want to edit.
2. Click **Edit**.



3. Make your changes and tap **Additional Details** to edit billing and additional information, or just

tap **Save Changes**.



See Also: Check In to Meetings and Invite People.

CHAPTER 45: Skype for Business Integration in EMS Mobile App

The EMS integration of Skype for Business in the Mobile App allows users to easily incorporate instant messaging and audio/video conferencing to their meetings without the need for A/V support. Skype for Business Integration is currently available for the EMS Mobile App, EMS Web App, and EMS for Outlook.

Important!

When considering using the Skype for Business Integration, keep in mind the following

- Skype for Business Integration is **ONLY** available on **Exchange-enabled templates**.
- **Users cannot edit or remove Skype for Business meetings from their reservations. Users can delete the link, but the Join link will remain enabled.**

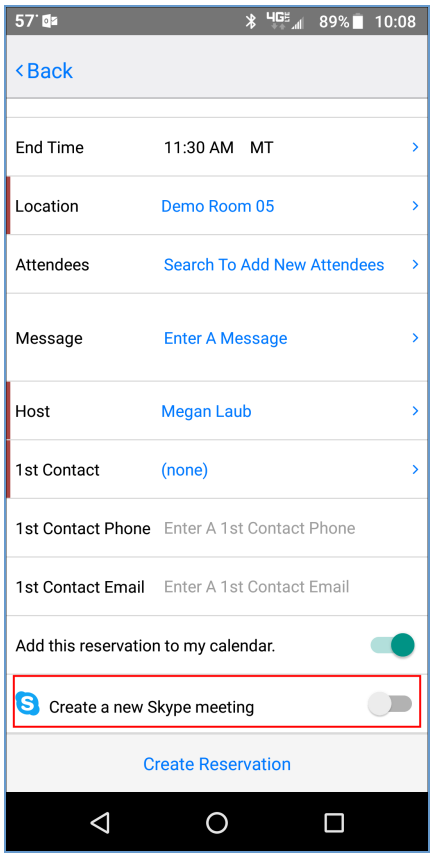
For more information about Configuring Skype for Business, see Configure Skype for Business.

This topic provides information about the following:

Add Skype for Business to a Reservation

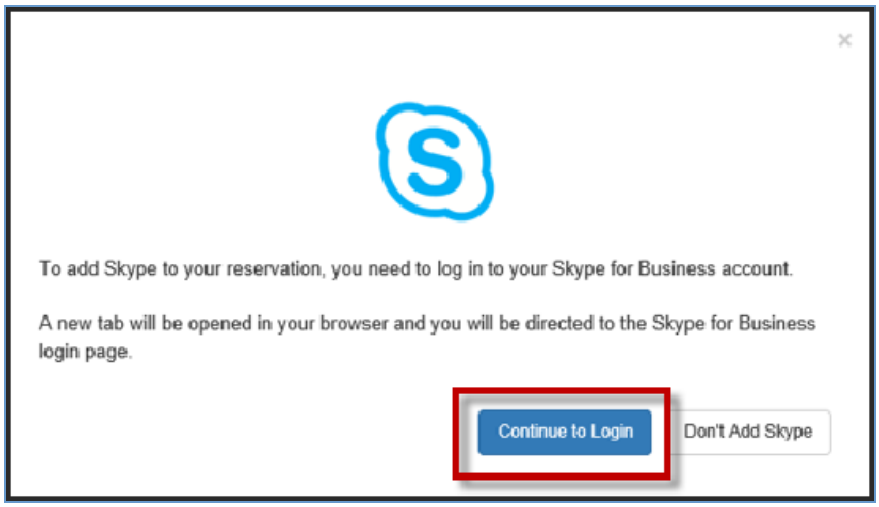
To add Skype for Business to a reservation in EMS Mobile App:

1. Sign in to your EMS Mobile App.
2. Create your reservation. Select a room and invite attendees.
3. At the bottom of the screen, there is a **Create a New Skype Meeting** toggle.



Skype for Business Toggle

4. If this is your first time using Skype for Business, an authentication form will appear. Sign in using your Skype credentials.
    - If your Skype account is authenticated, you can continue creating your reservation.
    - If your Skype account is not authenticated, an authentication modal will appear.
    - If you fail to authenticate your Skype account, the Skype toggle will be disabled.



Skype Authentication Form

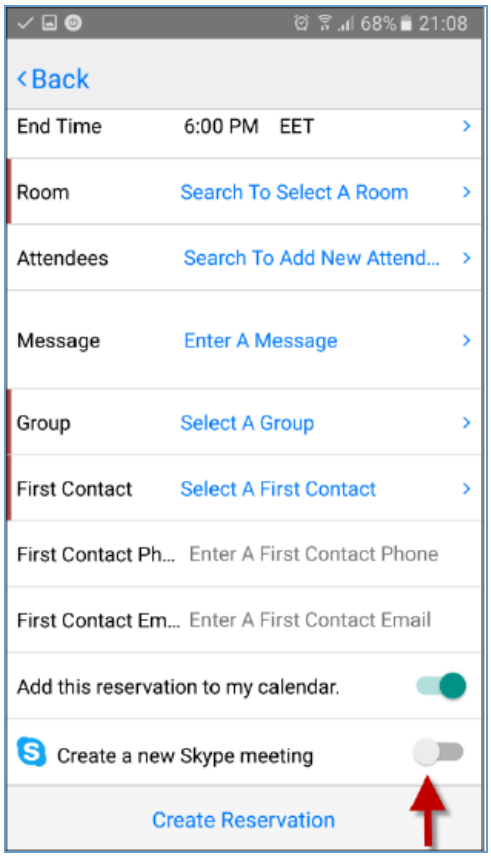
Note:

Authentication to Skype is dependent upon the deployment type. There are three deployment types for Skype for Business:

a. **On Premise:** This deployment for Skype for Business does not retain a token and requires authentication every 8 hours. As a result, you will be asked to sign in every 8 hours.
b. **Online:** This deployment retains the token so only an initial authentication is required.
c. **Hybrid:** This deployment has the same authentication method as the Online deployment.

For more information regarding authentications in Skype for Business, see Skype for Business Deployment Types.

5. Following authentication, slide the **Create a new Skype Meeting** toggle to add Skype for Business to your reservation.

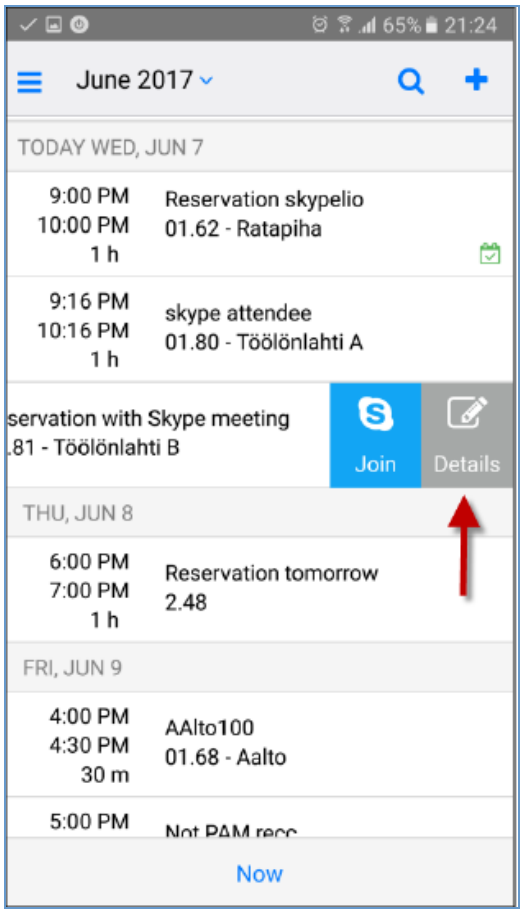


Create a New Skype Meeting Toggle

6. After successful authentication, you should receive a message that Skype has been successfully added to your reservation. To remove Skype from your reservation, slide the **Create a new Skype Meeting** toggle to the disabled position.
7. Click **Create Reservation**. Skype meeting information will appear in your meeting invitation and will be stored on the EMS database.

> **Important!**
> Once you have added Skype to your reservation, the meeting attendees will receive an email notification including the Join Skype link and call-in information.

8. Meeting hosts can view reservation details, including Skype meeting information, by navigating to the **Home** page. Swipe to the left of the meeting you want to view and click **Details**.



Select Details to View Skype Meeting Information

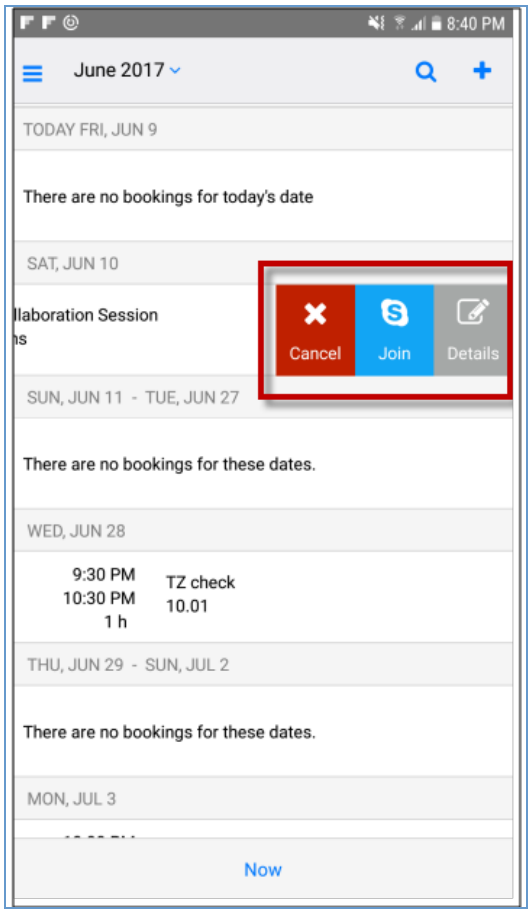
Note:

Once Skype has been added to your meeting, the Skype meeting information will appear in all EMS applications that have been integrated with Skype for Business (i.e., EMS for Outlook and EMS Web App).

Join a Skype for Business Meeting

To join a Skype for Business meeting in EMS Mobile App:

1. From the Home page, navigate to the meeting you want to attend. Swipe left. From this drawer, you will be able to **Cancel**, **Join**, and view **Details**.



Skype Join Meeting Button

2. Click **Join** to be connected to your Skype meeting.

For more information regarding using Skype for Business in other EMS access points, see also:

- Skype for Business in EMS for Outlook
- Skype for Business in EMS Web App

For more information regarding features of Skype for Business, refer to the Microsoft Skype for Business User Guide.

EMS Mobile App - April 2019

Accruent, LLC

11500 Alterra Parkway

Suite 110

Austin, TX 78758

www.accruent.com