



EMS MOBILE APP

Installation Guide

V44.1

Last Updated: January 16, 2018

Table of Contents

- EMS MOBILE APPInstallation Guide 1
- Table of Contents 2
- EMS Mobile AppInstallation Guide13
 - Contact Customer Support14
- Introduction 15
 - System Requirements for EMS Mobile App15
 - EMS Mobile or EMS Mobile Web App: What's the Difference? 16
 - EMS Mobile App = EMS Application for Mobile Devices17
 - Features of EMS Mobile App (Which are Not in EMS Web App) 17
 - EMS Mobile App = EMS Web App on a Mobile Browser 17
 - Features of EMS Web App (Which are Not in EMS Mobile App) 18

How Do I Install It?	18
How Do I Use It?	19
Installation and Basic Setup	22
Install EMS Platform Services on Your Web Server	22
Initial Configuration	25
Enable Everyday User Booking Templates	28
Architecture	31
Data Flow	31
Authentication	32
How EMS Mobile App Data Is Stored on Devices	35
Data at Rest	35
Encryption	37
Lifecycle	37

Sign In	37
Sign Out	41
System Requirements	42
What's New	44
Designed for Everyday Users on the Go	44
EMS Mobile App Features Not in EMS Web App	45
EMS Web App Features Not in EMS Mobile App	46
What's New in the Update 9 Release	46
Performance: Changes to the Technology Stack	46
Functionality	47
Integrated Authentication Options	48
Introduction	50
What is Integrated Windows Authentication?	52

What is Portal or Federated Authentication?	53
What is LDAP Authentication?	54
Contact Customer Support	57
Integrated Authentication Considerations	58
LDAP Integration	58
Pros	59
Cons	59
Integrated Authentication	59
Pros	60
Cons	60
Portal Authentication	60
Integrated Windows Authentication	62
Activate Integrated Windows Authentication for IIS 6.0	64

Activate Integrated Windows Authentication for IIS 7.x/8.x	66
Manage Everyday Users For Integrated Authentication	68
Manual Everyday User Account Creation	68
Automatic Everyday User Account Creation	70
EMS Web App Parameters	70
Portal/Federated Authentication Parameters	71
HR Toolkit (for EMS Workplace, EMS Campus, EMS Enterprise, EMS District, and EMS Legal only)	73
Automatic Template Assignment to Users	73
Existing Everyday User Accounts	74
LDAP Authentication	76
Overview	76
Configure EMS Web App to Use LDAP Authentication	79

Configure EMS Web App Security	81
Configure Communication Options	83
Core Properties	85
Non-AD Configuration	86
LDAP Queries	88
Save Your Configuration	89
Test Your Configuration	90
Configure Authentication for EMS Mobile App	91
Portal or Federated Authentication	92
Portal Authentication Overview	92
Installation/Configuration	94
Redirect User Log In to Your SSO Provider	96
Specify a Different Default Home Page for Guest Users	96

Portal Authentication Methods	98
Server Variable Method (Header Variable)	99
Server Variable Method - Federated (SAML)	100
Method 1: Locally installed Service Provider	100
Method 1 configuration Steps	101
Method 2	101
Method 2 Configuration Steps	102
EMS Configuration	102
Session Method	103
Form Method	105
Cookie Method	106
Query String Method	108
Authentication Options for EMS Mobile	109

Configure EMS Mobile Authentication	110
EMS Native Authentication	111
Test Your EMS Native Authentication	112
LDAP Authentication	113
Configure Your LDAP Provider	116
Configure EMS Web App to Use LDAP Authentication	119
Configuring EMS Web App Security	122
Configuring Communication Options	124
Core Properties	125
Non-AD Configuration	127
LDAP Queries	128
Save Your Configuration	129
Test Your Configuration	130

Configuring Authentication for the EMS Mobile App	131
Test Your LDAP Configuration	132
Test Your LDAP Authentication	133
Open ID Connect Authentication	135
Register Your EMS Mobile App with idP	136
Customize Your Configuration	136
Create a Configuration File	137
Use Hosted Configuration	137
Pre-Configure EMS Mobile App	138
Test Your Open ID Connect Configuration	138
Test Your Open ID Connect Authentication	139
Open ID Connect Authentication Can Be Hosted or Pre-Configured in the EMS Mobile App	141

How Users Authenticate After Configuration	142
How the Identity Provider (IdP) Works	143
How the EMS Platform Services API Works	144
Persistent Authentication	145
SAML Authentication	148
Configure SAML Authentication for EMS Mobile App	149
Identify Your Provider in Configuration	149
How EMS Platform Services Supports SAML	154
Use Hosted Configuration (Public Deployment)	155
Pre-Configure EMS Mobile App (Private Deployment)	156
Test Your SAML Configuration	156
Test Your SAML Authentication	157
SAML Authentication Can Be Hosted or Pre-Configured in the EMS	159

Mobile App	
How Users Authenticate After Configuration	160
How the Identity Provider (IdP) Works	161
How the EMS Platform Services API Works	162
Windows Authentication (NTLM) for EMS Mobile	163
User Login Scenario	163
Test Your Windows Authentication	164



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 may want to:

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

EMS Mobile App uses your phone's hardware features. You can use your phone's camera to scan a QR code to book or check-in to meetings.

Administrators can set a proximity-based check-in distance so that users



will be able to check-in to their meeting when they are within a certain distance of the building.

CONTACT CUSTOMER SUPPORT

- » **Option 1 (Recommended):** Submit a Ticket directly via the EMS Support Portal.
- » **Option 2:** Email support@emssoftware.com.
- » **Option 3 (Recommended for critical issues only):** Phone (800) 288-4565

Important: If you do not have a customer login, register [here](#).



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.

SYSTEM REQUIREMENTS FOR EMS MOBILE APP

The EMS Mobile App—which includes the EMS Platform Services—has specific requirements on top of the general EMS server and database 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.



Supported Platforms

Android 4.4, 5.0, 6.0

iOS 9.x, 10.x, 11.x

Prerequisites

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

- » EMS database server, web server and Platform Services (see [Requirements](#))
- » Mobile phone(s)

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 (WHICH 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 (WHICH ARE NOT IN EMS MOBILE APP)

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

HOW DO I INSTALL IT?

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

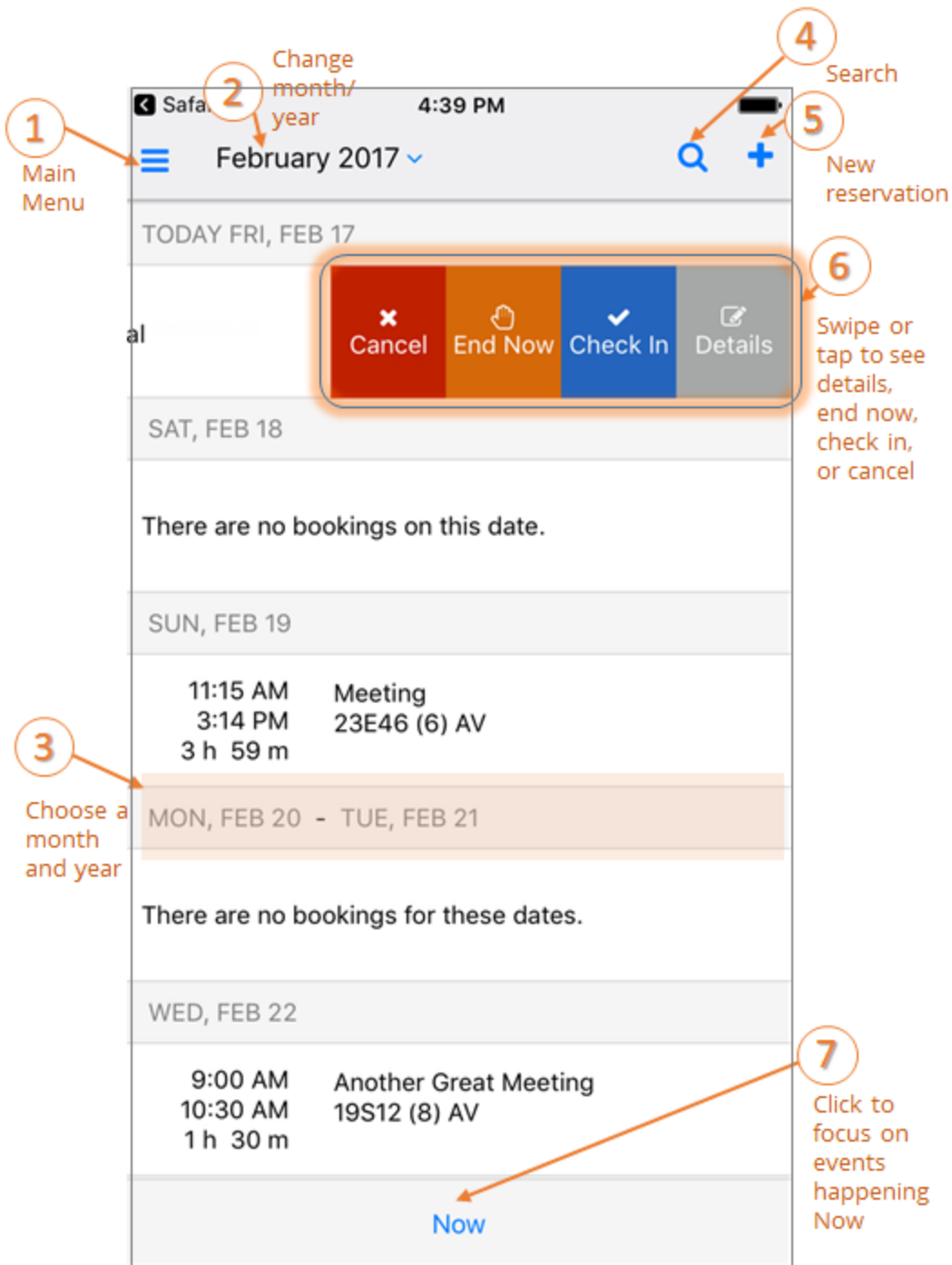
1. Download the installation files from the [EMS Customer Portal](#).
2. Install EMS Platform Services and connect to your organization's web server.
3. Set up user authentication.



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.

HOW DO I USE IT?

Once you've [logged in](#), you can follow the tips below to interact with your calendar and see your events. Your calendar shows only current and upcoming events.





Installation and Basic Setup

This topic provides instructions on how to do the following:

- » [Install EMS Platform Services on Your Web Server](#)
- » [Initial Configuration](#)
- » [Installation and Basic Setup](#)

See Also: [System Requirements](#)

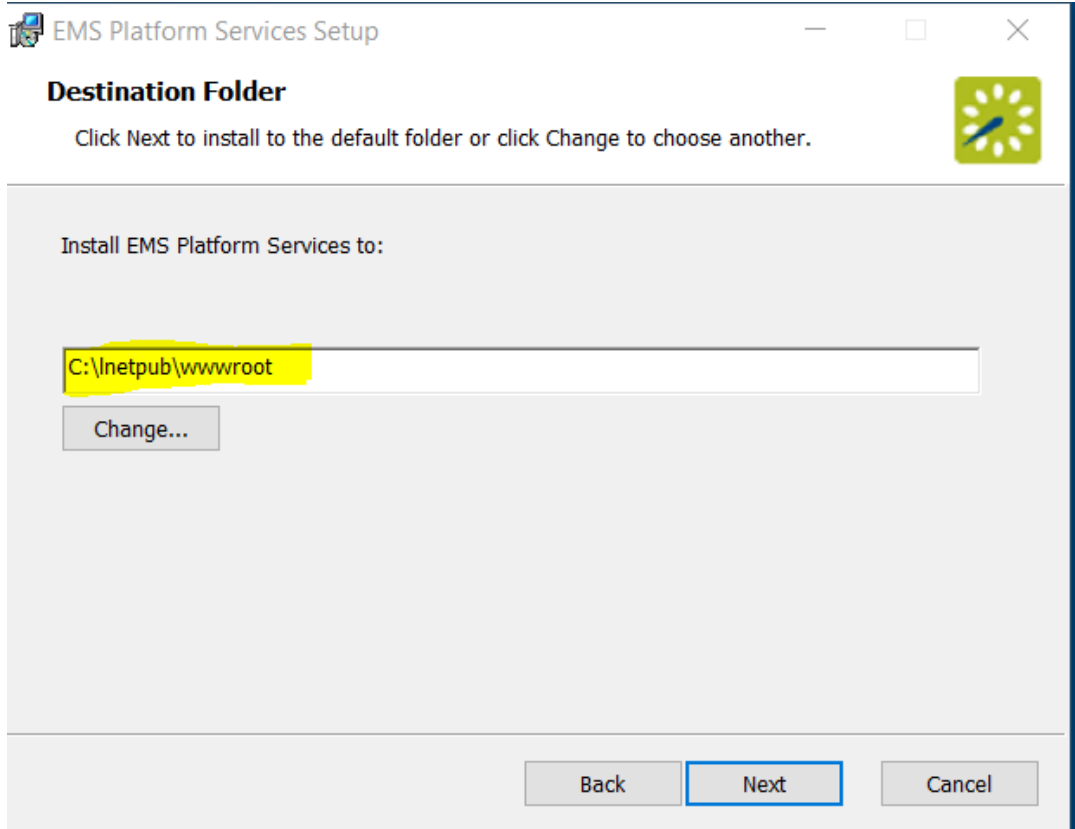
INSTALL EMS PLATFORM SERVICES ON YOUR WEB SERVER

1. Navigate to the [EMS Customer Portal](#). Log in, and in the Downloads area, locate EMS Platform Services.
2. Download the EMSPlatformServices.msi file.



3. Run this file 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.



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



INITIAL CONFIGURATION

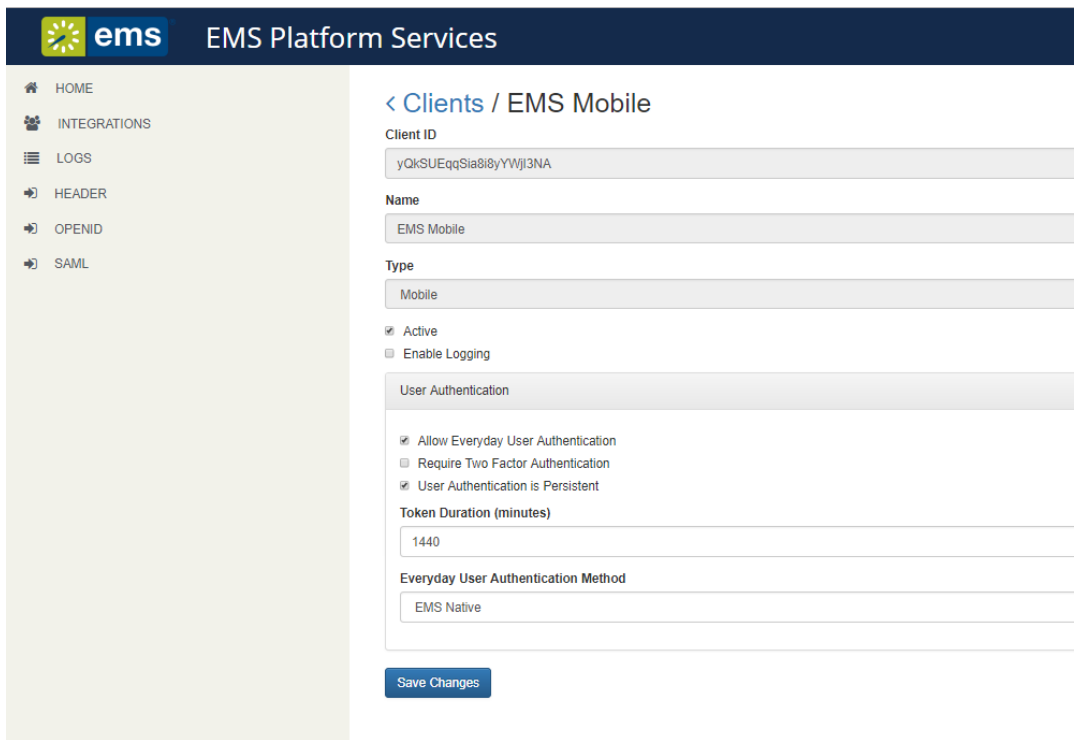
1. Access URL for EMS Platform Services

(e.g., <https://yourcompany.com/ems-platform-api>).

2. Log in using your credentials depending on your authentication type.

Please refer to [configuring Platform Services in the Admin Portal](#) for more details.

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



The screenshot shows the EMS Platform Services interface. On the left is a sidebar with navigation links: HOME, INTEGRATIONS, LOGS, HEADER, OPENID, and SAML. The main content area is titled "< Clients / EMS Mobile". It contains the following fields and options:

- Client ID**: yQkSUEqgSia8I8yYVWjl3NA
- Name**: EMS Mobile
- Type**: Mobile
- ☒ Active
- ☐ Enable Logging
- User Authentication**
 - ☒ Allow Everyday User Authentication
 - ☐ Require Two Factor Authentication
 - ☒ User Authentication is Persistent
- Token Duration (minutes)**: 1440
- Everyday User Authentication Method**: EMS Native
- Save Changes** button

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](#)
- » [Windows Authentication \(NTLM\) for EMS Mobile](#)
- » [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 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 [Deploy the EMS Mobile App](#) for more information.

ENABLE EVERYDAY USER BOOKING TEMPLATES

EMS V44.1 allows you to select which process templates (e.g., "web process templates") will be enabled on your users' mobile devices. From the Admin page for templates in the EMS Desktop Client, you will see an **Enable for Mobile** checkbox on the first tab of the template dialog box:

Process Template	Booking Rules	Defaults	Rooms	Categc
Description:	<input type="text" value="Workspace"/>			
Mode:	<input type="text" value="Self Serve"/>			
Menu Text:	<input type="text" value="Workspace"/>			
Available To New Users:	<input checked="" type="checkbox"/>			
Reserve Status:	<input type="text" value="Confirmed"/>			
Request Status:	<input type="text" value="Confirmed"/>			
Conflict Status:	<input type="text" value="Conflict"/>			
Cancel Status:	<input type="text" value="No Show"/>			
Rule Violation Status:	<input type="text" value=""/>			
Default Setup Type:	<input type="text" value="(none)"/>			
Menu Sequence:	<input type="text" value="0"/>			
Video Conference:	<input type="checkbox"/>			

Everyday User Application Settings

Enable for Web App:	<input checked="" type="checkbox"/>
Enable for Mobile:	<input checked="" type="checkbox"/>

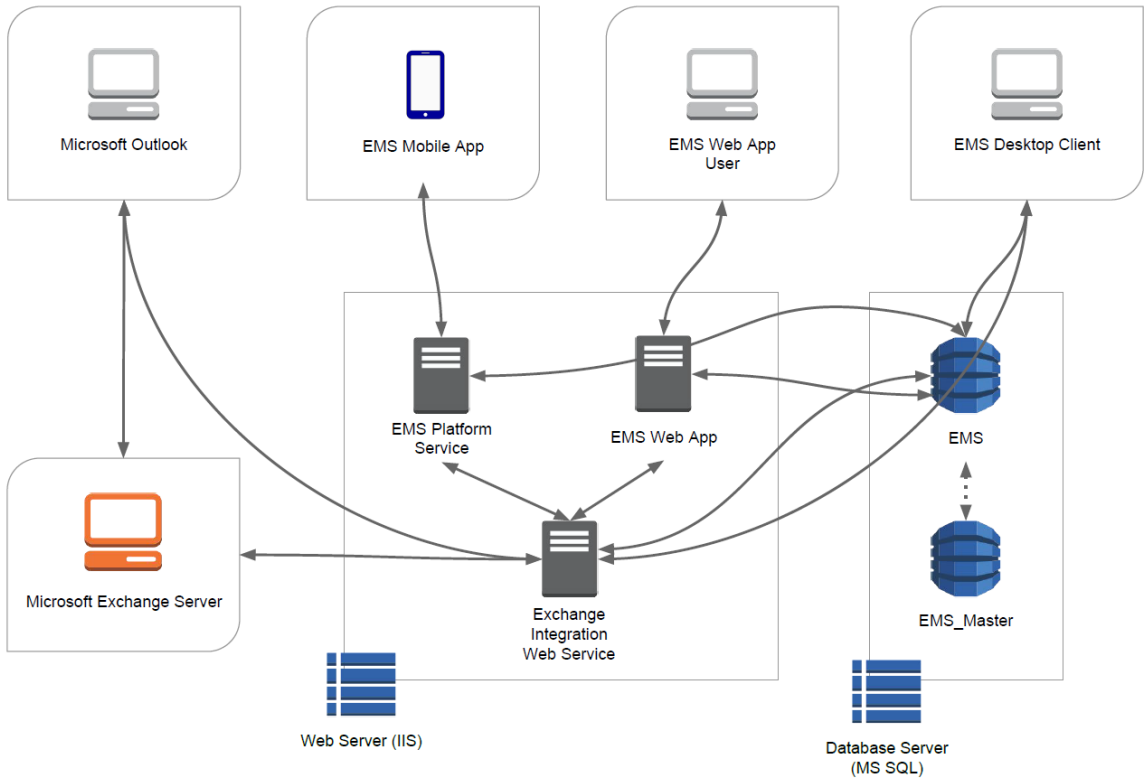
NOTE: EMS Mobile App is designed to make and edit simple reservations for users "on the go." At this time it cannot handle service requests, video conference bookings, or complex workflows. Please consider this when you decide which templates should be enabled for the EMS Mobile App. Additionally, you can only change the name and icon of the 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 mobile app.



Architecture

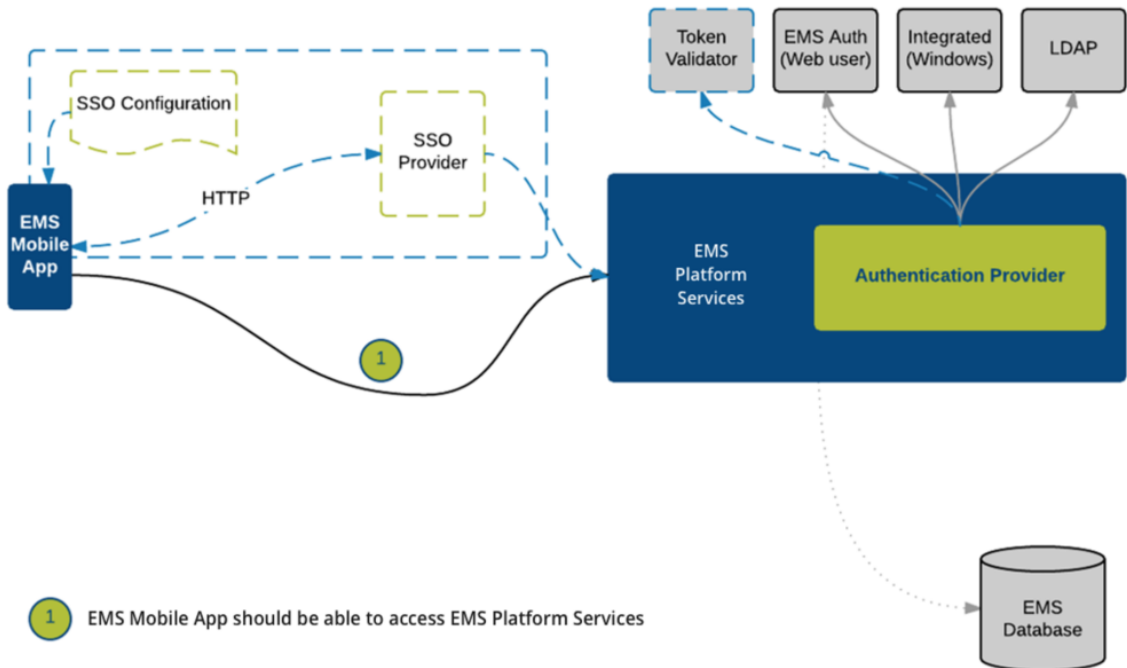
DATA FLOW

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.



© 2016 EMS Software, LLC

The EMS Mobile App consists of an iOS or Android native app deployed on users' smartphones, the EMS Mobile App API which sits on a web server, and the EMS database. The 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](#)



How EMS Mobile App Data Is Stored on Devices

This topic provides information on the following:

- » [Data at Rest](#)
- » [Encryption](#)
- » [Lifecycle](#)
- » [Sign In](#)
- » [Sign Out](#)

DATA AT REST

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

- » Per-feature data necessary for the application's functional and business goals:

- » Everyday User data (i.e., information about the current user)
- » Booking and Everyday User Process Template data
- » Favorite Rooms
- » Booking and Room details
- » Other similar feature-related data, subject to change over time

- » EMS Platform Services information, including version data and assorted parameter values required for operation
- » Application configuration data
- » Tokens for authentication:
 - » EMS Platform Services token
 - » Open ID token(s), if applicable

- » Device location information:
 - » Location information is stored to speed up certain location calculations that would severely impact performance if the application waited for the underlying OS to return the device's location

- » Application logs

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



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

ENCRYPTION

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

LIFECYCLE

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

SIGN IN

Following is an example response the EMS Platform Services API might send on successful authentication. This constitutes the personal



information stored in EMS Web App. Other data stored in the application is information related to that user, but is not information that identifies the user necessarily (i.e., the user's collection of Everyday User Process Templates and bookings, or favorites rooms).

This data is stored every time a user authenticates.

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

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

```
{  
  "userCount": 1,  
  "user": {  
    "userId": 1234,
```

```
"userName": "test",
"emailAddress": "test@emssoftware.com",
"externalReference": "",
"fax": "",
"networkId": "",
"phone": "",
"timeZoneId": 1,
"securityState": 0,
"validated": true,
"twoFactorState": null,
"allowAddGroup": true,
"allowAddContact": true,
"allowSetDefaultContact": true,
"webRoles": [
  {
    "type": 1,
    "code": "eventbrowser",
    "description": "Browse Events"
  }
]
```

```
],  
  "processTemplates": [  
    {  
      "id": 1,  
      "reserveStatusId": 1,  
      "requestStatusId": 2,  
      "conflictStatusId": 3,  
      "cancelStatusId": 4,  
      "allowPersonalization": true,  
      "mobileDeviceEnabled": true,  
      "webappEnabled": true,  
      "outlookEnabled": true  
    }  
  ],  
  "additionalProperties": null  
},  
  "trustedDeviceID": null,  
  "webToken": "eyJabc123.def456.ghi789" // example token  
}
```


SIGN OUT

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

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



System Requirements

The EMS Mobile App—which includes the EMS Platform Services—has specific requirements on top of the general EMS server and database 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.

SUPPORTED PLATFORMS

Android 4.4, 5.0, 6.0

iOS 9.x, 10.x, 11.x

Prerequisites

SUPPORTED PLATFORMS

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

- » EMS database server, web server and Platform Services (see [V44.1 System Requirements](#))
- » Mobile phone(s)



What's New

DESIGNED FOR EVERYDAY USERS ON THE GO

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

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

EMS Mobile App uses your phone's hardware features. You can use your phone's camera to scan a QR code to book or check-in to meetings.



Administrators can set a proximity-based check-in distance so that users will be able to check-in to their meeting when they are within a certain distance of the building.

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

EMS MOBILE APP FEATURES NOT IN EMS WEB APP

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



EMS WEB APP FEATURES NOT IN EMS MOBILE APP

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

WHAT'S NEW IN THE UPDATE 9 RELEASE

This release introduces several enhancements, summarized below. See Also: [Mobile App Release Notes for Update 9](#).

PERFORMANCE: CHANGES TO THE TECHNOLOGY STACK

- » EMS Mobile API to new Middle-tier product: EMS Platform Services (the first EMS application to consume RESTful API)
- » React Native framework for app development
- » Updated [Architecture](#)

FUNCTIONALITY

- » New user authentication options: new SSO authentication options, persistent authentication option, new EMS Mobile App Admin page
- » Create reservation: enhanced the filter for room search (now filters by Area, Building, Views, Capacity), smart defaults for start time and end time, time zone default to selected location
- » List view: removed past bookings, improved user interface improvements
- » Favorite rooms: added room filter



Integrated Authentication Options

This guide provides configuration instructions for System Administration and IT users for EMS Everyday User Applications: EMS Web App, EMS Mobile App, EMS for Outlook, and EMS Floor Plans.

This Integrated Authentication provides information on the following topics:

- » [Introduction](#)
 - » [Authentication Options for EMS Web App and Virtual EMS \(VEMS\)](#)
 - » [Authentication Options for EMS Mobile](#)
 - » [Authentication Options for EMS Master Calendar](#)
 - » [Authentication Options for EMS Regics](#)
- » [Integrated Authentication Considerations](#)
- » [Integrated Windows Authentication](#)
- » [Manage Everyday Users For Integrated Authentication](#)
- » [LDAP Authentication](#)



- » [Portal or Federated Authentication](#)
- » [Portal Authentication Methods](#)

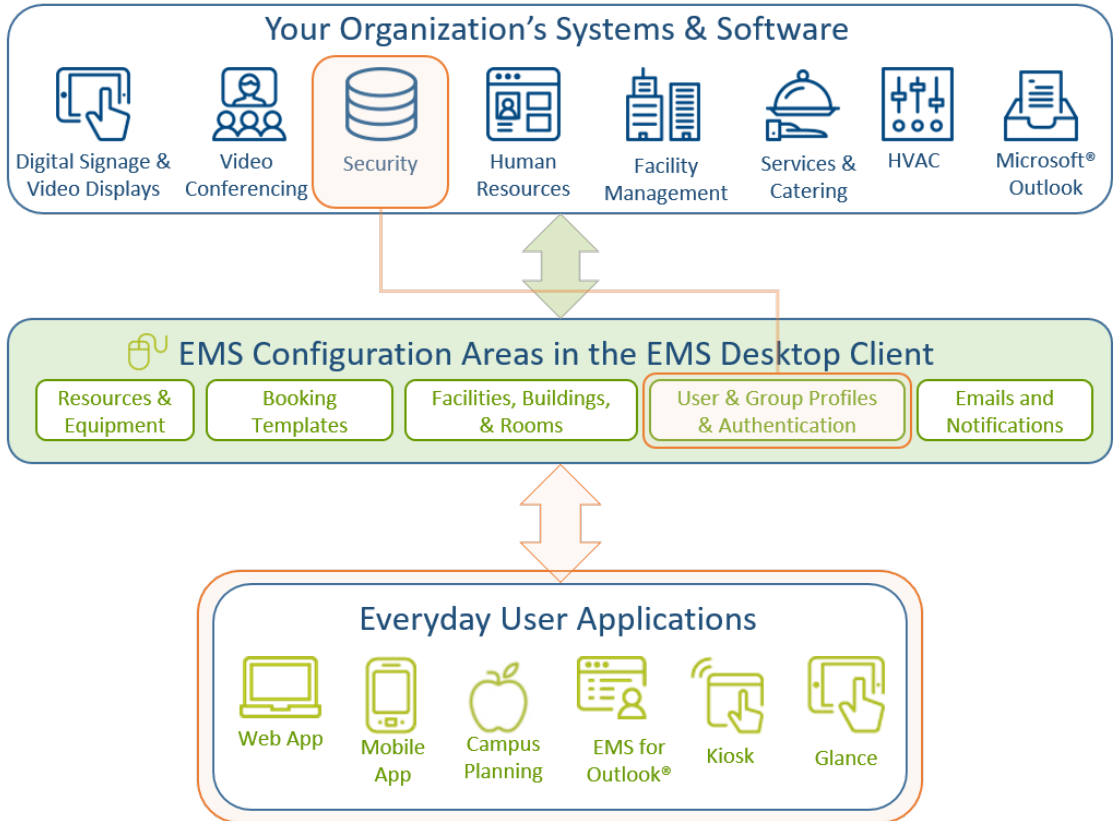


Introduction

The EMS Integrated Authentication component provides single-sign-on capability using Integrated Windows Authentication, your organization's portal, or LDAP. The Integrated Authentication Setup Guide lists the steps you must take to configure these Integrated Authentication options. If you are unsure whether your organization is licensed for Integrated Authentication or you would like to learn more about it, please contact your Account Executive.

The diagram below shows how your organizations' existing security software and systems integrate with EMS software applications through configurations you set in EMS Desktop Client.

Integration Diagram



When configuring integrated authentication using this component, you can use the following methods:

- » [Integrated Windows Authentication](#)
- » [Portal or Federated Authentication](#)
- » [LDAP Authentication](#)



WHAT IS INTEGRATED WINDOWS AUTHENTICATION?

Integrated Windows Authentication (IWA) is a built-in Microsoft Internet Information Services (IIS) authentication protocol that can be used to automatically authenticate and sign-in a user to EMS Web App. Integrated Windows Authentication works only with Internet Explorer and is best used on intranets where all clients accessing EMS Web App are within a single domain. When a domain user who is logged on to a networked PC accesses an EMS Everyday User application, such as EMS Web App, EMS Mobile App, or EMS for Outlook, their Active Directory credentials (Domain\User ID) are compared against corresponding Domain\User ID 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 automatically logged in.

For a more detailed explanation of the authentication methods outlined above, see [Integrated Windows Authentication](#).



WHAT IS PORTAL OR FEDERATED AUTHENTICATION?

The Portal Authentication method provides EMS Web App single sign-on capability using your organization's portal (e.g., CAS, Shibboleth, SiteMinder, Plumtree, uPortal, etc.). When a user logged into your portal accesses EMS Web App, a predefined user-specific variable (e.g., email address, employee/student ID, network ID, etc.) captured by your portal/sign-on page is compared against corresponding 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 automatically logged-into EMS Web App.

Note: The Field Used to Authenticate Everyday User parameter (within **System Administration > Settings > Parameters > Everyday User Applications** tab) is used by EMS Web App to determine which value should be used for authentication.



Several built-in authentication methods to pass-in credentials are available including:

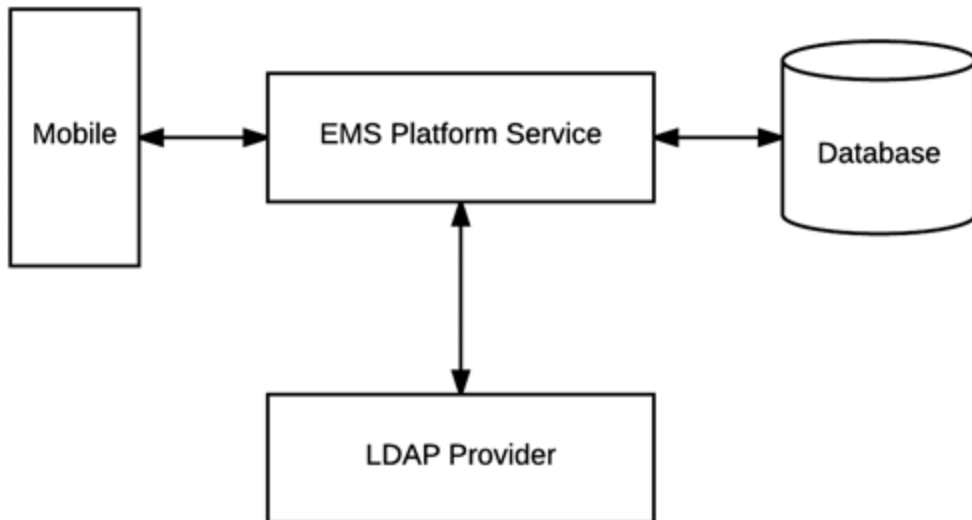
- » Server Variable (Header Variable)
- » Session
- » Form
- » Cookie
- » Query String
- » Federated (SAML)

For a more detailed explanation of the authentication methods outlined above, see [Portal Authentication Methods](#).

WHAT IS 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.



The LDAP Authentication topic covers the following information 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](#)

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.

Notes:

- » 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.

- » 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.

CONTACT CUSTOMER SUPPORT

- » **Option 1 (Recommended):** Submit a Ticket directly via the EMS Support Portal.
- » **Option 2:** Email support@emssoftware.com.
- » **Option 3 (Recommended for critical issues only):** Phone (800) 288-4565

Important: If you do not have a customer login, register [here](#).



Integrated Authentication Considerations

When you purchase the Integrated Authentication Service, you are able to use LDAP Integration, Integrated Authentication (IA), or Portal Authentication. Integrated and Portal Authentications are true Single Sign-On (SSO) solutions; LDAP is not. These methods are not typically used together. This section explains how each one works, along with pros and cons for each method.

LDAP INTEGRATION

LDAP integration allows you to bypass creating individual web users for your organization. By configuring EMS to query your LDAP groups, you can use LDAP groups to assign web template permissions. Your users would just use their windows credentials to login to the site. After creating a web user account (most data is pre-populated from their LDAP



account), they receive the template permissions granted to their LDAP group.

PROS

- » No need to create/maintain individual accounts for web users. Mass assign process templates.

CONS

- » Requires LDAP groups to be precisely defined and maintained to ensure proper access. EMS does not create or update LDAP groups, so product may require assistance from LDAP/Exchange administrators.
- » NOT Single Sign-on: users must enter windows credentials on each visit.

INTEGRATED AUTHENTICATION

IA is SSO. For this to work, every user must have a web user account created (manually through client/virtual piece or using our HRToolkit module). In each web account, a network ID is added. When a user visits VEMS or EMS Web App, a call is made to the machine to retrieve the windows account signed in. It compares that value to the network ID field in



existing accounts, logging in users automatically. Permissions are assigned to the individual web user accounts.

PROS

- » Can be true SSO - the account creation and maintenance can be completely invisible to the end user. Not reliant on Exchange/LDAP administrators.

CONS

- » Requires active web user creation and maintenance: manually on the client side, manually through end-user input, or automatically through an HR feed.

PORTAL AUTHENTICATION

With Portal Authentication, user information is passed from your existing portal to records in EMS by cookie, session string or similar. Portal Authentication is true SSO when used with our supported methods.

Note: When you implement Integrated Authentication, your consultant will assist you with creating templates and web users during onsite training. If you are adding this module separately and need assistance with virtual configuration contact your account manager about purchasing training. This document is intended to explain the different authentication options available, so you can anticipate any configuration needs. If you choose LDAP Integration, you will need to create an administrator account and admin web template to access the configuration page. See the EMS Setup Guide for questions with creating that template. Using LDAP with IA or Portal Authentication requires each user be responsible for creating/verifying their account on the first visit; SSO isn't immediate. Portal authentication can be used with LDAP, but this is atypical in most portal environments since other credentialing is available.

Integrated Windows Authentication

Integrated Windows Authentication (IWA) is a built-in Microsoft Internet Information Services (IIS) authentication protocol that can be used to automatically authenticate and sign-in a user to EMS Web App. Integrated Windows Authentication works only with Internet Explorer and is best used on intranets where all clients accessing EMS Web App are within a single domain.

This topic provides information on the following:

- » [Activate Integrated Windows Authentication for IIS 6.0](#)
- » [Activate Integrated Windows Authentication for IIS 7.x/8.x](#)

Note: Integrated Windows Authentication is supported for [EMS Floor Plan \(V44.1 Update 11\)](#).



See Also:

- » [Integrated Authentication Overview](#)
- » For more information, please review the following Microsoft TechNet articles on IWA for IIS [6.0](#), [7.0](#), and [8.0](#).
- » [Connect Your Database Using Active Directory](#)

When a domain user who is logged on to a networked PC accesses an EMS Everyday User application, such as EMS Web App, EMS Mobile App, or EMS for Outlook, their Active Directory credentials (Domain\User ID) are compared against corresponding Domain\User ID 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 automatically logged in.

Note: The Field Used to Authenticate Web User parameter (within **System Administration > Settings > Parameters > Everyday User Applications** tab is used to determine which value should be used for

authentication.

ACTIVATE INTEGRATED WINDOWS AUTHENTICATION FOR IIS 6.0

1. On the web server that hosts your EMS application's site, open **IIS Manager**.
2. Locate your EMS application's site.
3. Right-click your EMS application's site and choose **Properties**. The Properties screen will open.
4. Go to the **Directory Security** tab and click the **Edit** button under the Authentication and access control section. The Authentication Methods screen will open.
5. Uncheck the **Enable anonymous access** option. The **Integrated Windows**

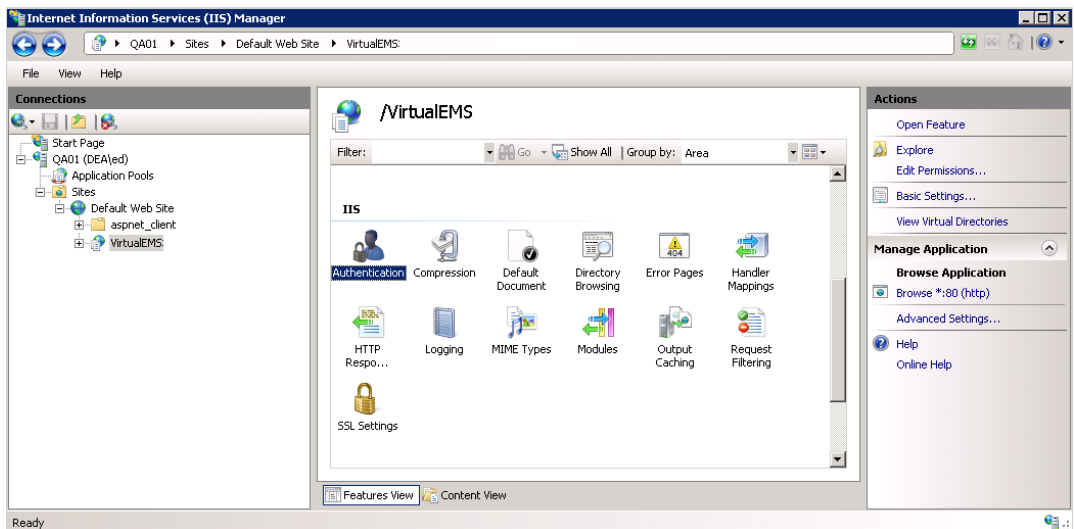


authentication option should be the only option checked.

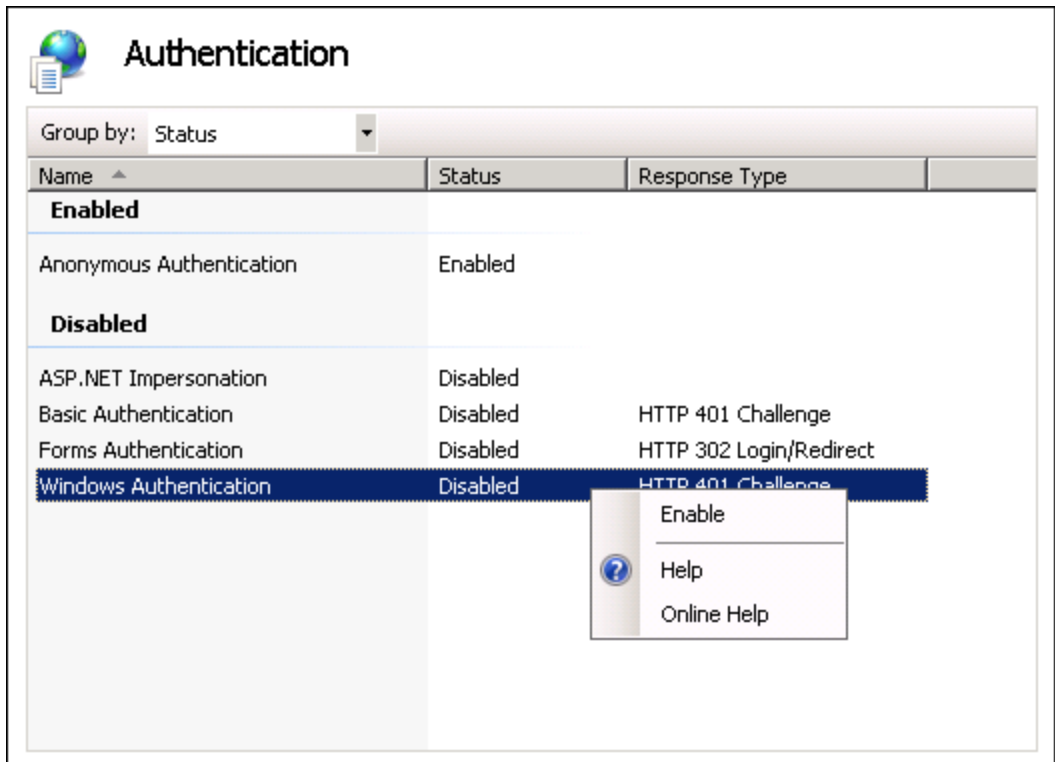
6. Click **OK** to exit the Authentication Methods screen. Click **OK** again to exit the Properties screen. You have completed the necessary IIS configuration steps for IIS 6.0.

ACTIVATE INTEGRATED WINDOWS AUTHENTICATION FOR IIS 7.X/8.X

1. On the web server that hosts your EMS application's site, open **IIS Manager**.
2. Locate and highlight your EMS application's site.



3. Double-click the **Authentication** option in the **IIS** section.



4. Right-click the **Windows Authentication** option and select **Enable**.
5. Right-click the **Anonymous Authentication** option and select **Disable**.
6. You have completed the necessary IIS configuration steps for IIS 7.



Manage Everyday Users For Integrated Authentication

In order to make a reservation in EMS Everyday User Applications, such as EMS Web App, EMS Mobile App, and EMS for Outlook, a user must have an active Everyday User account with appropriate security and process templates.

You can create Everyday User accounts within EMS in several ways:

- » [Manually Create Everyday User Accounts](#)
- » [Automatically Create Everyday User Accounts](#)
- » [Modify Existing Everyday User Accounts](#)

MANUAL EVERYDAY USER ACCOUNT CREATION

Everyday User accounts can be created manually by EMS Administrators within EMS Desktop Client or by anonymous Everyday Users on their



respective EMS Everyday Applications.

To create Everyday User accounts in the EMS Desktop Client, see [Configure Everyday Users](#).

To configure EMS Web App to allow anonymous Everyday Users to request an account, you adjust parameters. See also: [EMS Web App System Parameters](#).

Important: When manually creating an Everyday User account in an Integrated Authentication environment, you must specify a value in the Everyday User Network ID field or the External Reference field.

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



AUTOMATIC EVERYDAY USER ACCOUNT CREATION

Various configuration settings are available to automatically create Everyday User records (and assign the appropriate Security and Process Template(s) if applicable) when a user accesses an EMS Everyday User Application (such as EMS Web App for the first time).

EMS WEB APP PARAMETERS

Within the Everyday User Applications parameters area of the EMS desktop client (**System Administration > Settings > Parameters > Everyday User Applications** tab), the following parameters must be set accordingly:

AREA	DESCRIPTION	VALUE
Account Management	Auto Create Everyday User Account (for Integrated Authentication)	Yes



AREA	DESCRIPTION	VALUE
Account Man- agement	Default Security Template for User	<i>Must be specified</i>
Account Man- agement	Default Account Status for Newly- Created User	Active

PORTAL/FEDERATED AUTHENTICATION PARAMETERS

For organizations using Portal or Federated authentication, EMS supports a simple account provisioning strategy. When using Auto Create, EMS requires that a Everyday User account is provisioned with a name, an email address and a NetworkId (some authentication key). Otherwise, the user will be redirected to the Account Management page and be asked to manually enter the required information. In addition to the required fields, EMS also supports collecting phone, fax, and an external reference value. The parameters below are meant to help create a more



complete Everyday User. The values for each of the parameters are to be determined by the information populated by your portal.

AREA	DESCRIPTION	VALUE
Authentication	Portal Authentication Email Variable	<i>Must be specified</i>
Authentication	Portal Authentication External Reference Variable	<i>Must be specified</i>
Authentication	Portal Authentication Fax Variable	<i>Must be specified</i>
Authentication	Portal Authentication Name Variable	<i>Must be specified</i>
Authentication	Portal Authentication Phone Variable	<i>Must be specified</i>



HR TOOLKIT (FOR EMS WORKPLACE, EMS CAMPUS, EMS ENTERPRISE, EMS DISTRICT, AND EMS LEGAL ONLY)

The HR Toolkit is an optional component that allows you to automate the creation and maintenance of Everyday User records in EMS using an outside employee data source like your HR system or another data store within your organization. Please refer to the [HR Toolkit Installation Instructions](#) for information. If you are not licensed for the HR Toolkit, but would like to learn more about it, please contact your Account Executive.

AUTOMATIC TEMPLATE ASSIGNMENT TO USERS

The Default Security Template for User parameter shown above is used to automatically assign the correct Everyday User Security Template to new Everyday User records.

You can automatically assign default Everyday User Process Templates when a new Everyday User account is created. To automatically assign a Everyday User Process Template to new Everyday Users, select



the Available to New Everyday Users option within your Everyday User Process Template(s) (**Configuration > Everyday User Applications > Everyday User Process Templates (Edit the template > Process Templates tab)**)).

EMS customers using the LDAP Authentication method can use an alternate method to assign a Everyday User Process Template to a Everyday User based on the LDAP Group(s) to which the user belongs. This approach can be used in addition to or in lieu of the Everyday User Process Template assignment approach discussed above. Please see the [LDAP Authentication](#) section for configuration instructions.

EXISTING EVERYDAY USER ACCOUNTS

Warning for Existing EMS Customers: Before activating any Integrated Authentication option, the **Network ID** field or **External Reference** field must be populated on all existing Everyday User records. Ignoring this step may result in duplicate Everyday User records.

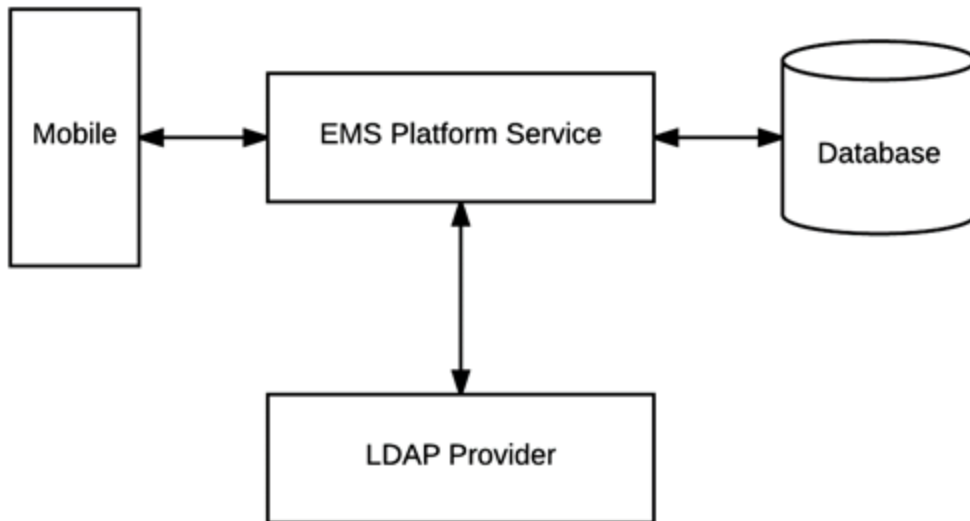




LDAP Authentication

OVERVIEW

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.



This topic provides information on the following:

- » [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](#)

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.

Notes:

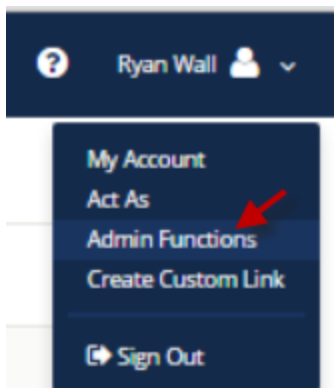
- » The EMS Web App LDAP-Process Template assignment process requires that your implementation of LDAP stores group information (e.g., staff, student, department, etc.) as a Directory Service object containing a property (i.e., member) that contains the users that belong to your various groups.
- » The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

CONFIGURE EMS WEB APP TO USE LDAP AUTHENTICATION

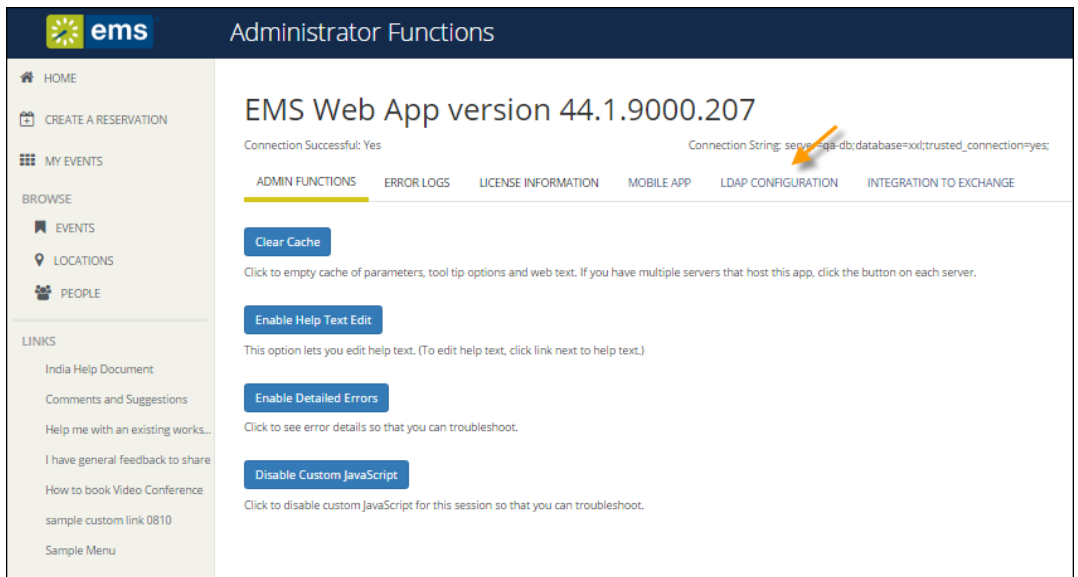
1. Log into EMS Web App with a User that belongs to an Everyday User Security Template containing the **Web Administrator** role (controlled in the EMS Desktop Client under **Configuration > Everyday User Applications > Everyday User Security Templates**).

See Also: [Configure Security Templates](#)

2. From the User Options, select **Admin Functions**.



3. Then click the **LDAP Configuration** tab.



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

ems

LDAP Configuration

?

Ryan Wall

HOME

CREATE A RESERVATION

MY EVENTS

BROWSE

EVENTS

LOCATIONS

PEOPLE

LINKS

Georgia

Alabama

Security

Communication Options

Core Properties

Non-AD Config

LDAP Queries

Test Configuration

See "VEMS Integrated Authentication Install.PDF" for instructions on how to configure these settings. If you're not familiar with 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 LDAP configuration can be tested on the Test Configuration tab.

☒

Authenticate users via LDAP?

☒

Authenticate mobile users via LDAP?

☒

Use LDAP to assign Process Templates - uncheck this to just use LDAP for authentication

☐

Use advanced communication options (requires Communication Options configuration, typically NOT required for Active Directory)

Path for LDAP Query Example: LDAP://yourdomain.com (NOTE: You probably need to have "LDAP" in all caps). If using Communication Options, leave the LDAP:// off (i.e. yourdomain.com:port)

LDAP://dea.com

List of Domains Separate with a comma, leave blank if in a single domain environment or in an environment where specifying domain for authentication is unnecessary

LDAP DomainUser The user id of the account Virtual EMS will use when contacting Directory Services

dea@andrzejdacka

LDAP Password Supply only if you are updating (NOTE: It will be stored in an encrypted format)

Authentication Type Some directory services don't implement Secure binding. FastBind is a pretty common authentication type.

Secure

Save

CONFIGURE EMS WEB APP SECURITY

1. On the **Security** tab:

- Select the **Authenticate users via LDAP** checkbox to enable LDAP authentication.

- b. If LDAP will be used to assign Everyday User Process Templates to your Web Users, select the **Use LDAP to assign Process Templates** checkbox.
- c. **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.
- d. In the **Path for LDAP Query** field, specify a valid LDAP path (example - LDAP://YourCompany.com)
- e. **List of Domains:** Skip this step if your organization uses a single domain. Otherwise, provide a comma separated list of your domains.
- f. In the **LDAP Domain\User** field, enter a Domain User account that has rights to query LDAP (example - YourDomain\User)
- g. In the **Password** field, enter a valid Password for the User Account entered in the previous step.
- h. 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

Warning: 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

Warning: 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

Warning: 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

Warning: 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 be 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, proceed to Step 7. Otherwise, you have completed the configuration process.

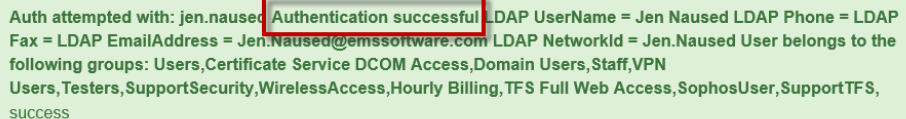
2. Within EMS Desktop Client, go to the Everyday User Process Templates area (**Configuration > Web > Everyday User Process Templates**).



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).



Auth attempted with: jen.naused **Authentication successful** LDAP UserName = Jen Naused LDAP Phone = LDAP Fax = LDAP EmailAddress = Jen.Naused@emssoftware.com LDAP NetworkId = Jen.Naused User belongs to the following groups: Users,Certificate Service DCOM Access,Domain Users,Staff,VPN Users,Testers,SupportSecurity,WirelessAccess,Hourly Billing,TFS Full Web Access,SophosUser,SupportTFS, success



- 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.

CONFIGURE AUTHENTICATION FOR EMS MOBILE APP

1. If your organization uses EMS Mobile App, click the **Mobile App** tab.
2. [Choose the LDAP option.](#)

Portal or Federated Authentication

This topic provides information on the following:

- » [Portal Authentication Overview](#)
- » [Installation/Configuration](#)
 - » [Redirect User Log In to Your SSO Provider](#)
 - » [Specify a Different Default Home Page for Guest Users](#)

PORTAL AUTHENTICATION OVERVIEW

The Portal Authentication method provides EMS Web App single sign-on capability using your organization's portal (e.g., CAS, Shibboleth, SiteMinder, Plumtree, uPortal, etc.). When a user who is logged into your portal accesses EMS Web App, a predefined user-specific variable (e.g., email address, employee/student ID, network ID, etc.) captured by your portal/sign-on page is compared against corresponding 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 automatically logged-into EMS Web App.

Note: The Field Used to Authenticate Everyday User parameter (within **System Administration > Settings > Parameters > Everyday User Applications** tab) is used by EMS Web App to determine which value should be used for authentication.

Several built-in authentication methods to pass-in credentials are available including:

- » Server Variable (Header Variable)
- » Session
- » Form
- » Cookie
- » Query String
- » Federated (SAML)

For a more detailed explanation of the authentication methods outlined above, see [Portal Authentication Methods](#).

INSTALLATION/CONFIGURATION

1. Within the Everyday User Applications parameters area of EMS (System Administration > Settings > Parameters (Everyday User Applications tab), the following parameters must be set accordingly:

AREA	DESCRIPTION	VALUE
Authentication	Portal	Required if Portal Authentication
	Authentication	Method = Cookie
	Cookie Key	
Authentication	Portal	Server Variable
	Authentication	
	Method	Session
		Form

AREA	DESCRIPTION	VALUE
		Cookie
		Query String

Authentication	Portal	User variable to be compared
	Authentication	against the EMS Everyday
	Variable	User External Reference/Network ID field

2. Direct users to the default EMS Web App page. If the default installation settings were used, the default page is:

([http://\[ServerName\]/EMSWebApp/Default.aspx](http://[ServerName]/EMSWebApp/Default.aspx))

(replace [ServerName] with the name of your web server)

REDIRECT USER LOG IN TO YOUR SSO PROVIDER

Administrators can hide the login form on the My Home page and instead, present a single **Sign In** button that links to the override URL. Open the web.config file and locate the following code to customize the redirect:

```
<!--<add key="loginOverrideUrl" value=""/>-->
```

Additionally, you can do the same for user log out:

```
<!--<add key="logoutOverrideUrl" value=""/>-->
```

Changing the URL in these areas means that when users log in or out, they will pass through your SSO provider.

SPECIFY A DIFFERENT DEFAULT HOME PAGE FOR GUEST USERS

Additionally, you can now [specify a different site home page](#) for unauthenticated users.



Portal Authentication Methods

This topic provides information about the following:

- » [Server Variable Method \(Header Variable\)](#)
- » [Server Variable Method - Federated \(SAML\)](#)
 - » [Method 1: Locally installed service provider](#)
 - » [Method 2](#)
- » [EMS Configuration](#)
 - » [Session Method](#)
 - » [Form Method](#)
 - » [Cookie Method](#)
 - » [Query String Method](#)

Note: EMS applications do not natively support SAML. You must use our [Portal Authentication](#) to use SAML.



SERVER VARIABLE METHOD (HEADER VARIABLE)

Server Variable/Header Variable is a collection of variables that are set by Internet Information Server (IIS).

Applications like SiteMinder create custom server variables for portal site use.

Code example:

Set the **Portal Authentication Method** parameter to Server Variable and type the appropriate variable for the **Portal Authentication Variable** parameter. Direct users to your EMS Web App Default.aspx page.



SERVER VARIABLE METHOD - FEDERATED (SAML)

SAML can be leveraged for authentication with your EMS applications by leveraging our portal authentication method and a service provider of your choosing.

METHOD 1: LOCALLY INSTALLED SERVICE PROVIDER

Using this method, you install a service provider of choice on the web-server hosting the EMS web applications. All traffic is routed through that service provider (typically via an ISAPI filter). This service provider will manage all of the authentication for the user. Once the user has successfully authenticated, it will pass an identifier for the user to the EMS application using one of our portal methods. In this scenario typically the Server Variable (Header) method is used.



METHOD 1 CONFIGURATION STEPS

1. Install and configure a service provider on the EMS web server
2. Set the service provider to protect the specified EMS web applications
3. Configure the service provider to pass the required user attributes
4. In EMS, configure the EMS Web App parameter “Portal Authentication Method”
5. In EMS, configure the applicable Portal Authentication Variables.

METHOD 2

This method can be common if there is already a server configured with a service provider in your environment, handling authentication for other applications. In EMS you can configure your application to re-direct any login requests to the other server to be authenticated. Once the user is authenticated, the server with your service provider installed sends the user back to the EMS Application with an identifier for the user in the header, or within a cookie. The EMS application reads this header, or cookie value, and leverages portal authentication to sign the user in with the matched credentials.



METHOD 2 CONFIGURATION STEPS

1. Install and configure a service provider on the EMS web server
2. Set the service provider to protect the specified EMS web applications
3. Configure the service provider to pass the required user attributes
4. In EMS, configure the EMS Web App parameter “Portal Authentication Method”
5. In EMS, configure the applicable Portal Authentication Variables.
6. In EMS, change the Login URL under **Configuration > Everyday User Applications > Web App Menus**.
 - a. Select **Login.aspx** and click **Edit**
 - b. Enter in the URL to your Remote Service Provider
7. Configure your remote Service provider to send the user back to the default.aspx page of the web application that the request originated from.

EMS CONFIGURATION

Please reference our Portal Authentication section for further details around the configuration required within EMS. There are a number of different options available. You will need to know the method that the user



identifying value will be passed and the name of that value. Other values can also be passed (ie: email address and phone number) to aid in automatic web user account provisioning as well.

SESSION METHOD

A session is a way to provide/maintain user state information in an inherently stateless environment. It provides access to a session-wide cache you can use to store information.

In order to use the session method, set the Portal Authentication Method parameter to **Session** and type the appropriate variable for the Portal Authentication Variable parameter. Then you must create an asp.net web page and name it with the .aspx extension similar to the example below. The asp.net web page created must be copied into the EMS Web App root web directory. It must be copied there in order for EMS Web App to read the session variable.

You will need to pass through the user's email address or external reference to your asp.net web page.



Code example in vb.net:

```
<%@ Import Namespace="System" %>
```

```
<script runat="server" language="vb">
```

```
    Sub Page_Load(ByVal sender As System.Object, ByVal e As System.EventArgs)
```

```
        Session.Item("EMS Web AppSession") = "test@ems-software.com"
```

```
        Response.Redirect("Default.aspx")
```

```
    End Sub
```

```
</script>
```




FORM METHOD

Forms enable client-side users to submit data to a server in a standardized format via HTML. The creator of a form designs the form to collect the required data using a variety of controls, such as INPUT or SELECT. Users viewing the form fill in the data and then click Submit to send the data to the server.

To use the form method, set the Portal Authentication Method parameter to **Form** and type the appropriate variable for the Portal Authentication Variable parameter. To create portals through a form, create a web page with a form similar to below. Once the user logs on through the portal, the form below can be submitted to log the user on to EMS Web App.

Code example in HTML:

```
<Form name="form1" method="Post" action=" http://[ServerName]/  
EMSWebApp/Default.aspx ">
```



```
<input type="hidden" id="EMS Web AppFORM" name="EMS  
Web AppFORM" value="test@emssoftware.com">
```

```
<input type="submit" value="submit">
```

```
</form>
```

COOKIE METHOD

A cookie is a small piece of information stored by the browser. Each cookie is stored in a name/value pair called a crumb—that is, if the cookie name is "id" and you want to save the id's value as "this", the cookie would be saved as id=this.

You can store up to 20 name/value pairs in a cookie, and the cookie is always returned as a string of all the cookies that apply to the page. This means that you must parse the string returned to find the values of individual cookies. Cookies accumulate each time the property is set. If you try to set more than one cookie with a single call to the property, only the first cookie in the list will be retained.



To use the cookie method, set the Portal Authentication Method parameter to **Cookie** and type the appropriate variable for the Portal Authentication Cookie Key parameter. Then create a web page with code similar to below. Once the user logs on through the portal, take their user logon information and create a cookie. After the cookie is created send the user to your EMS Web App Default.aspx page.

Code example in Active Server Pages 2.0:

```
<%@LANGUAGE="VBSCRIPT" %>
```

```
<%
```

```
    Response.Expires = -1
```

```
    Response.Cookies("EMS Web AppCookie")("CookVal") =  
    "test@emssoftware.com"
```

```
    Response.Cookies("EMS Web AppCookie").Path = "/"
```



```
Response.Cookies("EMS Web AppCookie").Expires = DateAdd  
("m", 3, Now)
```

```
Response.Redirect("http://[ServerName]/ EMSWe-  
bApp/Default.aspx ")
```

```
%>
```

QUERY STRING METHOD

A query string is information appended to the end of a page's URL. An example using portal authentication is below.

Code example:

```
http://[ServerName]/ EMSWe-  
bApp/Default.aspx?MCQS=test@emssoftware.com
```

To use the query string method, set the Portal Authentication Method parameter to **Query String** and type the appropriate variable for the Portal Authentication Variable parameter.



Authentication Options for EMS Mobile

System Administrators only need to have administrative privileges to EMS Desktop Client (including EMS Web App settings) in order to control setup for the EMS Mobile App. All settings for EMS Web App also control booking behavior and "Everyday User" access and booking templates in EMS Mobile App.

See Also:

- » [EMS Mobile App System Parameters](#)
- » [Configuring QR Codes](#)
- » [Setting Up EMS Web App](#)
- » [EMS Mobile App Requirements](#)
- » [Installing EMS Mobile App](#)



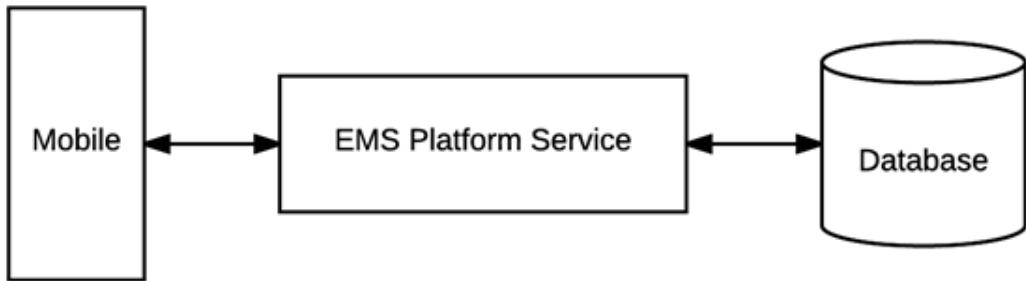
Configure EMS Mobile Authentication

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

- » [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](#)
- » [Configure EMS Mobile Authentication](#)
- » [Windows Authentication \(NTLM\) for EMS Mobile](#)

EMS Native Authentication

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



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

- » Enter his or her credentials on the Sign In screen.
- » Tap **Sign In**.
- » 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/ems-platform-api>), 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.



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.

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:

- » [Configuring EMS Web App to Use LDAP Authentication](#)
- » [Configuring EMS Web App Security](#)
- » [Configuring Communication Options](#)



- » [Core Properties](#)
- » [Non-AD Config](#)
- » [LDAP Queries](#)
- » [Saving Your Configuration](#)
- » [Testing Your Configuration](#)
- » [Configuring Authentication for EMS Mobile App](#)

CONFIGURE YOUR LDAP PROVIDER

1. Navigate to Platform Services admin portal (<https://yourcompany.com/ems-platform-api>) and select Integrations from the sidebar. Select EMS Mobile and choose LDAP from everyday user authentication method dropdown.

- HOME
- INTEGRATIONS
- LOGS
- HEADER
- OPENID
- SAML

< Clients / EMS Mobile

Client ID

yQkSUEqqSia8i8yYWjI3NA

Name

EMS Mobile

Type

Mobile

☒ Active

☐ Enable Logging

User Authentication

☒ Allow Everyday User Authentication

☐ Require Two Factor Authentication

☒ User Authentication is Persistent

Token Duration (minutes)

1440

Everyday User Authentication Method

EMS Native

EMS Native
Header

LDAP

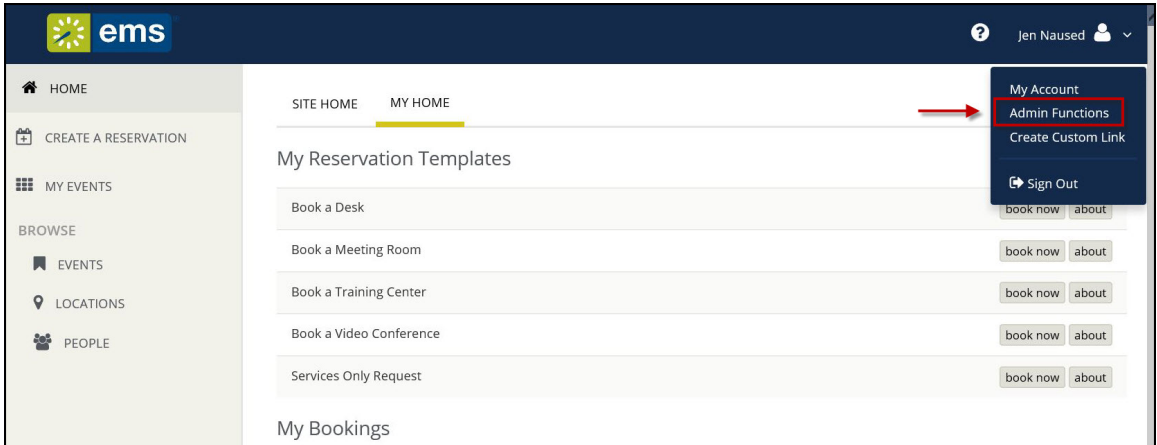
NTLM

Open ID

SAML



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



3. Tap the **LDAP Configuration** tab and complete all required LDAP information, and then [Test Your LDAP Configuration](#).



Administrator Functions ? Ankita Verma

HOME
 CREATE A RESERVATION
 MY EVENTS
BROWSE
 EVENTS
 LOCATIONS
 PEOPLE

EMS Web App version 44.1.12000.448

Connection Successful: Yes Connection String: server=ems01;database=emshq_book;

ADMIN FUNCTIONS ERROR LOGS LICENSE INFORMATION LDAP CONFIGURATION INTEGRATION TO EXCHANGE

Clear Cache

Click to empty cache of parameters, tool tip options and web text. If you have multiple servers that host this app, click the button on each server.

Enable Help Text Edit

This option lets you edit help text. (To edit help text, click link next to help text.)

Enable Detailed Errors

Click to see error details so that you can troubleshoot.

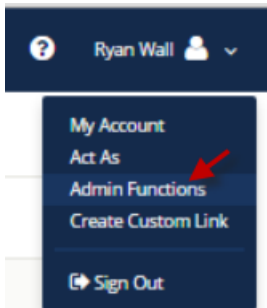
Tip: This is the same process you use for [LDAP Authentication](#). The EMS Platform Services API uses the same configuration information.

CONFIGURE EMS WEB APP TO USE LDAP AUTHENTICATION

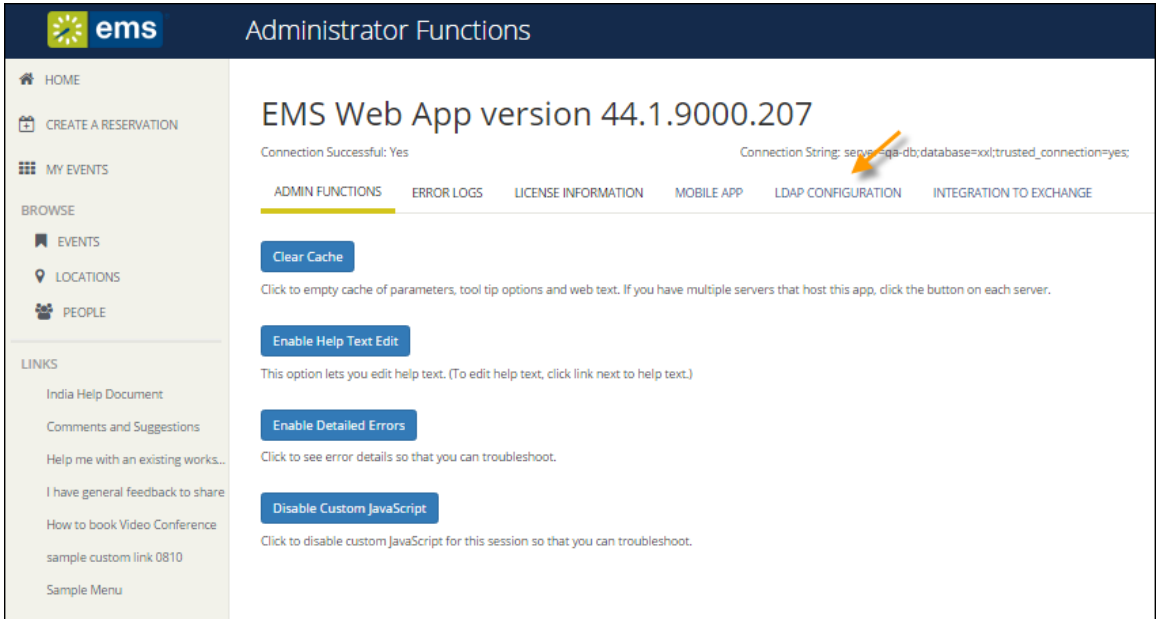
1. Log into EMS Web App with a User that belongs to an Everyday User Security Template containing the Web Administrator role (controlled in the EMS Desktop Client under Configuration > Everyday User Applications >

Everyday User Security Templates). See Also: Configuring Security Templates

2. From the User Options, select Admin Functions.



3. Click the LDAP Configuration tab.



Administrator Functions

EMS Web App version 44.1.9000.207

Connection Successful: Yes Connection String: server=qa-db;database=xxl;trusted_connection=yes;

ADMIN FUNCTIONS ERROR LOGS LICENSE INFORMATION MOBILE APP LDAP CONFIGURATION INTEGRATION TO EXCHANGE

Clear Cache

Click to empty cache of parameters, tool tip options and web text. If you have multiple servers that host this app, click the button on each server.

Enable Help Text Edit

This option lets you edit help text. (To edit help text, click link next to help text.)

Enable Detailed Errors

Click to see error details so that you can troubleshoot.

Disable Custom JavaScript

Click to disable custom JavaScript for this session so that you can troubleshoot.

HOME

CREATE A RESERVATION

MY EVENTS

BROWSE

EVENTS

LOCATIONS

PEOPLE

LINKS

India Help Document

Comments and Suggestions

Help me with an existing works...

I have general feedback to share

How to book Video Conference

sample custom link 0810

Sample Menu

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

ems

LDAP Configuration

?

Ryan Wall

▼

HOME

CREATE A RESERVATION

MY EVENTS

BROWSE

EVENTS

LOCATIONS

PEOPLE

LINKS

Georgia

Alabama

Security

Communication Options

Core Properties

Non-AD Config

LDAP Queries

Test Configuration

See "VEMS Integrated Authentication Install.PDF" for instructions on how to configure these settings. If you're not familiar with 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 LDAP configuration can be tested on the Test Configuration tab.

☒ Authenticate users via LDAP?

☒ Authenticate mobile users via LDAP?

☒ Use LDAP to assign Process Templates - uncheck this to just use LDAP for authentication

☐ Use advanced communication options (requires Communication Options configuration, typically NOT required for Active Directory)

Path for LDAP Query Example: LDAP://yourdomain.com (NOTE: You probably need to have "LDAP" in all caps). If using Communication Options, leave the LDAP:// off (i.e. yourdomain.com:port)

LDAP://dea.com

List of Domains Separate with a comma, leave blank if in a single domain environment or in an environment where specifying domain for authentication is unnecessary

LDAP DomainUser The user id of the account Virtual EMS will use when contacting Directory Services

dea/andrzej.dacka

LDAP Password Supply only if you are updating (NOTE: It will be stored in an encrypted format)

Authentication Type Some directory services don't implement Secure binding. FastBind is a pretty common authentication type.

Secure

Save

CONFIGURING EMS WEB APP SECURITY

1. On the Security tab:
 - a. Select the Authenticate users via LDAP checkbox to enable LDAP authentication.
 - b. If LDAP will be used to assign Everyday User Process Templates to your Web Users, select the Use LDAP to assign Process Templates checkbox.

- c. 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.
- d. In the Path for LDAP Query field, specify a valid LDAP path (example - LDAP://YourCompany.com)
- e. List of Domains: Skip this step if your organization uses a single domain. Otherwise, provide a comma separated list of your domains.
- f. In the LDAP Domain\User field, enter a Domain User account that has rights to query LDAP (example - YourDomain\User)
- g. In the Password field, enter a valid Password for the User Account entered in the previous step.
- h. 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.

CONFIGURING COMMUNICATION OPTIONS

Warnings: 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

Warnings: 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

Warning: 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

Warning: 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 be 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, proceed to Step 7. 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).

Auth attempted with: jen.naused Authentication successful LDAP UserName = Jen Naused LDAP Phone = LDAP Fax = LDAP EmailAddress = Jen.Naused@emssoftware.com LDAP NetworkId = Jen.Naused User belongs to the following groups: Users,Certificate Service DCOM Access,Domain Users,Staff,VPN Users,Testers,SupportSecurity,WirelessAccess,Hourly Billing,TFS Full Web Access,SophosUser,SupportTFS, SUCCESS

- 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 e.g. <https://yourcompany.com/ems-platform-api>, then you can test the configuration with a simple curl command:

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

Tip: 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 critical 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://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.

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:

- » [Register Your EMS Mobile App with idP](#)
- » [Customize Your Configuration](#)
- » [Create a Configuration File](#)



- » [Test Your Open ID Connect Configuration](#)
- » [Test Your Open ID Connect Authentication](#)

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 endpoint.

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 may 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 and 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.

Warning: 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 wish 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://ems.yourcompany.com/endpoint/api/v1/health
```

Tip: 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.



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 may 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 may 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.

Persistent 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.

Tip: 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.

EMS Platform Services

HOME

INTEGRATIONS

ROLES

LOGS

HEADER

OPENID

SAML

CALENDARING

< Clients / EMS Mobile

Client ID

yQkSUEqqSia8I8yYVWj3NA

Name

EMS Mobile

Type

Mobile

Role

All Routes

☒ Active

☐ Enable Logging

☐ Allow this client to book without Everyday User Templates and ignore Booking Rules

User Authentication

☒ Everyday User Authentication Required

☐ Require Two Factor Authentication

☒ User Authentication is Persistent

Token Duration (minutes)

1440

Everyday User Authentication Method

EMS Native

Save Changes

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 [HR Toolkit](#) to streamline this process.



SAML Authentication

This section guides you authenticating your users with a SAML provider. Authentication with SAML requires getting configuration information into EMS Mobile App prior to beginning the authentication flow.

To use SAML authentication, you will:

1. [Configure SAML Authentication for EMS Mobile App](#)
2. [Test Your SAML Configuration](#)
3. [Test Your SAML Authentication](#)

Note: For more information about how SAML Authentication can be hosted or pre-configured in the EMS Mobile App, see [SAML Authentication Can Be Hosted or Pre-Configured in the EMS Mobile App](#).



CONFIGURE SAML AUTHENTICATION FOR EMS MOBILE APP

Setting up SAML involves configuration on both the Identify Provider and Service Provider sides.

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 may be needed in order to configure your IdP.

- » **EMS Platform Signing Certificate:** Optional certificate used by EMS Platform to sign AuthnRequests sent to IdP.
- » **SP Issuer:** Optional service provider identifier used to identify the EMS Platform to the identify provider. (e.g. <http://mycompany.com/EmsPlatform>)
- » **Service Provider Post back URL:** Optional URL for Identify Provider to use for generating SAMLResponse POST Back URL to EMS Platform as the Service Provider. This should be set to the URL to the EMS Platform Services



SAML Auth Endpoint (e.g., <https://mycompany.com/EmsPlatform/api/v1/authentication/saml>). If the Service Provider post back URL is not configured with the IdP, then it will need to be configured from the EMS Platform Admin UI.

» Following fields are required to complete SAML authentication configuration:

FIELD	DESCRIPTION
Form Post Field Name	HTTP Form Post Attribute (optional, default is Sam-IResponse). Attribute in which assertions are sent, within encoded <samlp:Response> document.
User Info Request Method	Dropdown with choice of assertion element containing user identity (NameID or Attribute). If set to Attribute, then must set Identity Attribute Name to expected assertion attribute name to use for user identity.
Identity Attribute	Assertion attribute name containing user identity. Attribute names can be identity provider specific (i.e. 'uid',

FIELD	DESCRIPTION
Name	'mail').
Identity Provider Issuer	Optional Identity Provider Issuer (i.e. urn:em-splayground.auth0.com) to use to verify expected issuer of assertions, included in SAMLResponse as <saml:Issuer>.
Service Provider Issuer	Optional Service Provider issuer identifier, to be included by EMS Platform in AuthnRequest requests sent to Identify Provider. This maps to the <saml:Issuer> element in the SAML AuthnRequest. Ex: http://-mycompany.com/EmsPlatform
Identity Provider URL for Service	Required Identity Provider Redirect URL (ex. https://id-p.example.org/SAML2/SSO/Redirect). This URL includes two SAML-defined query string argument (typically 'SAMLRequest' and 'RelayState'). 'SAMLRequest'

FIELD	DESCRIPTION
Provider Redirect	includes the authentication request details, provided by EMS Platform. 'RelayState' contains opaque data that EMS Platform includes in the request, in order for the Identify Provider to include as Relay State on the SAML Response. If 'SAMLRequest' and 'RelayState' are not included in the configured URL, the EMS Platform will add them automatically to the request sent to the Identify Provider. For example, if you configure a URL of https://id-p.example.org/SAML2/SSO/Redirect, the resulting URL that EMS Platform calls will look like https://id-p.example.org/SAML2/SSO/Redirect?SAMLRequest=[SamlRequest data]&RelayState=[Opaque EMS Data].
Service Provider Callback URL	Base URL of EMS Platform, used for the Identity Provider callback URL in the SAML HTTP POST binding. Set this URL to the base URL of the EMS Platform installation (i.e. https://mycompany.com/EmsPlatform).

FIELD	DESCRIPTION
Path to Identity Provider Public Certificate	Optional identity provider public key (.pem) for EMS Platform to use to verify SAML Assertions.
Path to Service Provider Public Certificate	Optional Customer-generated public cert (.cer/.pem) file containing base64 encoded public cert for EMS Platform to use to sign AuthnRequests sent to identity provider.
Path to Service Provider Private Certificate	Optional Customer-generated private cert (.cer/.pem) file containing base64 encoded public cert for EMS Platform to use to sign AuthnRequests sent to identity provider.

FIELD	DESCRIPTION
Private Cer- tificate	

HOW EMS PLATFORM SERVICES SUPPORTS SAML

No 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.

See Also: [Persistent Authentication](#) for token expiration configuration details. See Also: 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 may 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 (PUBLIC DEPLOYMENT)

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

Warning: 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 wish to pre-configure EMS Mobile App, see [Configure and Re-Sign the EMS Mobile App](#).

TEST YOUR SAML 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://ems-  
s.yourcompany.com/endpoint/api/v1/health
```

Tip: 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":"saml" // <-- these are the critical lines  
      "ui":"saml"  
    }  
  }  
}
```

TEST YOUR SAML AUTHENTICATION

The SAML process should be testable in a browser, assuming all configuration is correct.

1. Visit the EMS Platform Services API SAML URL in a browser: *<https://yourcompany.com/ems-platform...ntication/saml>*



2. After logging in a logging in as a user, you should see a JSON response in the browser containing the EMS Platform Services API's authentication response.



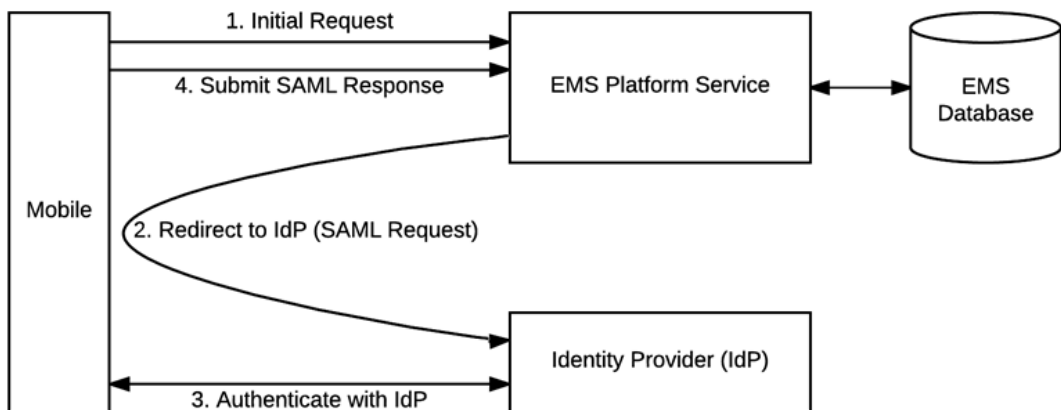
SAML Authentication Can Be Hosted or Pre-Configured in the EMS Mobile App

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.



- » User may briefly see a busy indicator while the page loads.

Users will authenticate using the SAML authorization view. They do not participate in the following steps (which explain the completion of the SAML flow). 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 it 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 `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.



Windows Authentication (NTLM) for EMS Mobile

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

Tip: 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:

- » EMS Mobile user will enter domain credentials on the Sign In screen and tap **Sign In**.
- » EMS Mobile App will send credentials to the EMS Platform Services API.



- » IIS will intercept the call and issue a challenge to EMS Mobile App.
 - » Mobile application will then perform all steps necessary to complete process with the user's provided credentials.
- » Platform API receive the initial request and extract the authenticated user from the IIS context.
- » Platform API will verify the authenticated user against the EMS database and respond to the mobile app.
- » EMS Mobile 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 Mobile App will inform the user.

TEST YOUR WINDOWS AUTHENTICATION

Assuming you have installed the EMS Platform Services API at <https://yourcompany.com/ems-platform-api>, 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.